

UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI SCIENZE GIURIDICHE (SCUOLA DI GIURISPRUDENZA)



**DOTTORATO DI RICERCA IN SCIENZE GIURIDICHE
XXXIV CICLO**

**TESI DI DOTTORATO IN SCIENZE GIURIDICHE
*curriculum internazionalistico-europeo-comparato***

***Mutuo riconoscimento e acquisizione dell'e-evidence
nello spazio di libertà, sicurezza e giustizia
tra vecchi e nuovi strumenti di cooperazione giudiziaria penale***

**Coordinatore:
Ch.mo Prof. *Geminello PRETEROSS***

**Candidato:
*Alessio GAUDIERI***

**Tutor:
Ch.ma Prof.ssa *Angela DI STASI***

**Matricola:
8800600057**

**Co-tutor
Ch.mo Prof. *Luigi KALB***

ANNO ACCADEMICO 2020-2021

L'uomo è nato libero e ovunque si trova in catene.

JEAN-JACQUES ROUSSEAU, *Il contratto sociale*, 1762

Alla mia *famiglia*,
perché,
nonostante le tante catene,
mi dà gli strumenti per *essere*
libero.



KAZIMIR SEVERINOVICH MALEVIČ, *Točil'schik Printsip Mel'kaniia* (L'Arrotino ovvero il Principio dello Scintillio), 1912-1913, olio su tela, Yale University Art Gallery.

“Le apparenze esteriori della natura non offrono alcun interesse; solo la sensibilità è essenziale”.

(KAZIMIR SEVERINOVICH MALEVIČ)

INDICE

CAPITOLO I INTRODUZIONE. IL CONTESTO SOCIO-GIURIDICO

1.	L'impatto delle nuove tecnologie nell'era digitale. Il processo di digitalizzazione.....	pag.	1
2.	La metamorfosi della criminalità transnazionale nell'era del digitale: fenomenologia della criminalità informatica organizzata e della criminalità informatica.....	»	9
2.1.	(Segue). Il <i>cyber</i> terrorismo.....	»	18
3.	Il cyberspazio come luogo di consumazione dei reati.....	»	26
3.1.	Da Internet... ..	»	26
3.2.	... al <i>cyberspace</i>	»	30
3.3.	<i>Deep web</i> e <i>Dark web</i>	»	32
3.4.	Il <i>cloud computing</i>	»	38
4.	Argomentazioni sul <i>locus commissi delicti</i> . La difficile applicazione dei criteri di giurisdizione e di competenza del giudice	»	41
5.	Il "dedalo" nozionistico della prova digitale e le sue caratteristiche	»	57
6.	La natura intrinsecamente transnazionale della prova digitale. Piano dell'opera	»	67

CAPITOLO II COOPERAZIONE GIUDIZIARIA IN MATERIA PENALE E MUTUO RICONOSCIMENTO

1.	La "sfida" della cooperazione giudiziaria in materia penale.....	pag.	76
1.1.	(Segue). La "quinta libertà" e la cooperazione giudiziaria come esigenza	»	81
2.	La disciplina della cooperazione giudiziaria in materia penale nell'Unione europea	»	82
3.	(Segue). La cooperazione "verticale" e la cooperazione "orizzontale"	»	86
4.	Le nuove sfide e gli sviluppi della cooperazione giudiziaria in materia penale nell'Unione europea	»	89
5.	Il principio della mutua assistenza e la progressiva riduzione della sua applicazione	»	102
6.	Il principio cardine della cooperazione giudiziaria tra Stati membri dell'Unione europea: il mutuo riconoscimento	»	105

INDICE

7.	Il mutuo riconoscimento quale presupposto per la “libera circolazione” delle decisioni giudiziarie	»	113
8.	La “fiducia reciproca” e il rispetto dei diritti fondamentali quali elementi necessari per il mutuo riconoscimento	»	118
9.	Il principio del mutuo riconoscimento tra uniformazione e armonizzazione	»	128
10.	L’inclusione del principio del mutuo riconoscimento nel Codice di procedura penale italiano. Il titolo I- <i>bis</i> del Libro XI del Codice di rito	»	133
11.	(Segue). La formulazione del nuovo art. 696- <i>bis</i> c.p.p.	»	140
12.	Il principio di equivalenza e il principio di proporzionalità nel sistema dell’Unione europea	»	142
13.	L’attenzione dell’Unione europea al tema della prova elettronica	»	149
14.	(Segue). Verso nuovi strumenti per la formazione della prova elettronica transnazionale	»	154

CAPITOLO III

LA CONVENZIONE EUROPEA SULLA CRIMINALITÀ INFORMATICA E LA COOPERAZIONE CON GLI USA

1.	La Convenzione del Consiglio d’Europa sulla criminalità informatica: un quadro generale	pag.	161
2.	La mutua assistenza per la formazione dell’ <i>e-evidence</i> secondo i principi generali individuati dalla Convenzione	»	171
3.	La mutua assistenza per la formazione dell’ <i>e-evidence</i> prevista dalla Convenzione sulla criminalità informatica in assenza di accordi internazionali applicabili	»	179
3.1.	La procedura	»	182
4.	L’oggetto della domanda di assistenza giudiziaria	»	195
5.	L’ingiunzione di produrre	»	208
6.	Luci ed ombre della Convenzione sulla criminalità informatica. Verso un Secondo protocollo	»	216
7.	I lavori preparatori del Secondo protocollo	»	220
8.	Il Secondo protocollo alla Convenzione sulla criminalità informatica	»	225
9.	Le procedure volte a migliorare la cooperazione diretta con fornitori ed enti privati di altre Parti. Elementi di comunanza ...	»	230
9.1.	La procedura per l’ottenimento di informazioni sulla registrazione del nome di dominio	»	232
9.2.	La divulgazione delle informazioni sugli abbonati	»	234
10.	Le nuove procedure di cooperazione internazionale tra autorità per la produzione di dati informatici	»	239
10.1.	L’ordine di produzione accelerata	»	241

INDICE

10.2.	La divulgazione accelerata di dati informatici in assenza di una richiesta di assistenza	»	245
11.	La mutua assistenza d'emergenza	»	248
12.	Le regole relative alla formazione della prova elettronica transfrontaliera vigenti negli Stati Uniti d'America	»	251
13.	I negoziati in vista di un Accordo tra l'Unione europea e gli Stati Uniti d'America	»	261

CAPITOLO IV

MUTUO RICONOSCIMENTO E LEGALE FORMAZIONE DELL'E-EVIDENCE

1.	La necessità di strumenti all'avanguardia per la legale formazione della prova elettronica transnazionale nell'Unione europea	pag.	271
2.	L'ordine europeo di indagine avente ad oggetto la prova elettronica	»	276
3.	L'inadeguatezza dell'ordine europeo di indagine: verso una disciplina dell'e-evidence transfrontaliera nello spazio di libertà, sicurezza e giustizia	»	293
4.	Gli ordini europei di produzione e conservazione: la scelta della fonte normativa	»	299
5.	La funzione e l'ambito di applicazione degli ordini europei di produzione e conservazione	»	308
6.	L'ordine europeo di conservazione	»	321
7.	L'ordine europeo di produzione	»	331
7.1.	(Segue). La procedura di riesame in caso di contrasto con il diritto di un Paese terzo	»	346
8.	L'intervento dell'autorità di esecuzione in caso di inottemperanza	»	351
9.	Il principio del "diritto a difendersi, ricorrendo effettivamente".	»	356

CAPITOLO V

RILIEVI CONCLUSIVI

1.	Sfide future in tema di e-evidence transnazionale	pag.	367
2.	Le comuni e nuove incertezze	»	370
3.	Sull'abbandono del principio di territorialità	»	372
4.	Il ruolo propulsivo dell'Unione europea: un'ambizione possibile	»	374

INDICE

5.	Secondo protocollo addizionale alla Convenzione sulla criminalità informatica e attività dell'Unione europea	»	377
6.	La vera "sfida" dell'Unione europea: l'efficienza degli ordini europei di produzione e di conservazione	»	378
7.	Ampliamento del diritto di difesa <i>versus</i> limitazione delle investigazioni difensive	»	382
8.	Tecnologia e diritti fondamentali. A lezione dai classici per possibili azioni bilanciate	»	385
 <i>Bibliografia</i>			 pag. 391

CAPITOLO I

INTRODUZIONE. IL CONTESTO SOCIO-GIURIDICO

Sommario: 1. L'impatto delle nuove tecnologie nell'era digitale. Il processo di digitalizzazione. – 2. La metamorfosi della criminalità transnazionale nell'era del digitale: fenomenologia della criminalità informatica organizzata e della criminalità informatica. – 2.1. (Segue). Il *cyber* terrorismo. – 3. Il cyberspazio come luogo di consumazione dei reati. – 3.1. Da Internet... – 3.2. ... al *cyberspace*. – 3.3. *Deep web* e *Dark web*. – 3.4. Il *cloud computing*. – 4. Argomentazioni sul *locus commissi delicti*. La difficile applicazione dei criteri di giurisdizione e di competenza del giudice. – 5. Il “dedalo” nozionistico della prova digitale e le sue caratteristiche. – 6. La natura intrinsecamente transnazionale della prova digitale. Piano dell'opera.

1. L'impatto delle nuove tecnologie nell'era digitale. Il processo di digitalizzazione

La rivoluzione cibernetica¹ ha segnato il destino dell'intero pianeta, contribuendo ai mutamenti socio-economici. Non si tratta più di vivere e ragionare secondo i vecchi schemi analogici, che pure sono sopravvissuti, piuttosto bisogna prendere consapevolezza di abitudini, ambizioni, *modus vivendi et operandi* alla luce di un nuovo processo di evoluzione economica e di industrializzazione della società basato sull'uso generalizzato dei mezzi elettronici e digitali.

Risulta evidente anche al *quisque de populo* come la società stia cambiando. Il progresso scientifico e tecnologico ha ampliato i confini della coscienza e della conoscenza, modificando gli assetti sociali e relazionali.

La tecnologia sta rivoluzionando la vita delle persone e, con esse, della società intera. Lo sviluppo tecnologico deve assumere una funzione servente: deve rivelarsi mezzo di sostegno in periodi straordinari ed ausilio in tempi ordinari. Lo scoppio di una pandemia mondiale anche solo negli anni '90 del secolo scorso avrebbe reso particolarmente gravoso, se non impossibile, la didattica a distanza, o la connessione, la collaborazione ed il coordinamento veloce e proficuo tra i centri di ricerca mondiali che si occupano dello sviluppo dei vaccini o di farmaci utili alla guarigione.

Cambiano i pericoli e cambiano le istanze securitarie provenienti dalle varie fasce della popolazione. Le nuove tecnologie fanno sorgere diritti di nuova generazione e

¹ Il termine “cibernetica” deriva dal greco κυβερνήτης (timoniere), la cui radice rimanda al verbo κυβερνάω (dirigere, governare). La prima attestazione si ha in Omero, Iliade, XXIII, 316, in relazione al nocchiero che guida la nave battuta dai venti. Il termine assume anche, per estensione, un significato metaforico che sta ad indicare colui che guida – o governa – una città o uno Stato. In Platone è attestato proprio con il significato più ampio di arte del governo, mediante l'espressione κυβερνητική τέχνη “*kybernetikè technè*”. Nel 1900 ha indicato un vasto programma di ricerca interdisciplinare consistente nello studio matematico unitario degli organismi viventi e, più in generale, di sistemi, sia naturali che artificiali. Il primo ad utilizzare questo termine fu nel 1948 il matematico N. WIENER nel suo libro *La cibernetica: Controllo e comunicazione nell'animale e nella macchina*, ove tracciò l'ambito di interesse e gli obiettivi della nuova disciplina.

comprimono o mostrano un volto sinora sconosciuto di diritti già noti. Se, ad esempio, in passato si richiedevano maggiori dispositivi per la sicurezza di pedoni e conducenti di automobili, oggi ci si chiede come questi stessi dispositivi tecnologici nel tempo sviluppatisi possano garantire diritti come la *privacy*, l'identità, la riservatezza dei dati personali sensibili. Si chiede, dunque, agli operatori del diritto di individuare un equo bilanciamento tra diritti ed interessi contrapposti, raggiungibile solo applicando correttamente il principio di ragionevolezza e proporzionalità.

Sebbene la tecnologia risulti essere un valido alleato dell'essere umano, il suo potere può essere utilizzato anche negativamente per raggiungere scopi riprovevoli come consumare reati. Infatti, il potere delle tecnologie informatiche non conosce confini fisici, geografici, temporali, «supera le barriere doganali, elimina le differenze culturali tra i popoli»². Si assiste ad un potere che ben può sospendersi in un limbo spazio-temporale in attesa di manifestare la sua vera portata una volta attivato dalla criminalità.

La tecnologia informatica ha ormai così pervaso la vita umana, da non consentire più all'uomo di escluderla. Tutto ci parla di digitalizzazione: dalla sanità, alla giustizia; dall'istruzione, all'agroalimentare, dai trasporti alla finanza. Tutto oggi può essere gestito con strumenti digitalmente avanzati³. L'economia, la democrazia e la società dipendono dagli strumenti digitali che devono essere sicuri ed affidabili⁴.

Ed è proprio in questi meandri che si annidano le spire di una criminalità spesso latente. Infatti, distruggere o occultare elementi di prova utili all'accertamento di un fatto-reato e l'attribuzione di esso ad un determinato autore è molto più semplice: tempi ridotti e spazi dematerializzati consentono al crimine di rendere nebulosa o impossibile la ricostruzione del fatto-reato da parte dell'autorità giudiziaria. D'altra parte, non va però taciuta la possibilità di poter “congelare” quanto avviene nel contesto digitale e nel mondo di *internet*, almeno per un periodo legalmente e preventivamente determinato.

² Con queste parole, T.E. FROSINI, *Libertè, Egalité, Internet*, II ed., Napoli, 2019, p. 52.

³ Solo una fiorente comunità che utilizza tecnologie digitali e dati può garantire all'Europa una posizione di *leader* mondiale nella definizione di un'economia digitale. La digitalizzazione offre grandi opportunità alle aziende affinché incrementino l'efficienza dei processi di produzione e la capacità di innovare prodotti e modelli di business. L'impiego di tecnologie rivoluzionarie avanzate, quali la *blockchain* e l'intelligenza artificiale (IA), il *cloud computing* e il calcolo ad alte prestazioni, può imprimere un notevole impulso alla loro competitività. Cfr., Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, “*Una strategia per le PMI per un'Europa sostenibile e digitale*”, COM(2020) 103 final.

Inoltre, le nuove tecnologie costituiscono un ottimo alleato delle strategie a tutela dell'ambiente. Le tecnologie digitali sono un fattore fondamentale per conseguire gli obiettivi di sostenibilità del *Green Deal* europeo in molti settori diversi. La Commissione europea si è impegnata ad esaminare misure finalizzate a garantire che le tecnologie digitali, quali l'intelligenza artificiale, il G5, il *cloud* e l'*edge computing*, nonché l'*Internet of things*, possano accelerare e massimizzare l'impatto delle politiche per affrontare i cambiamenti climatici e proteggere l'ambiente. La digitalizzazione presenta inoltre nuove opportunità per il monitoraggio a distanza dell'inquinamento atmosferico e idrico o per il monitoraggio e l'ottimizzazione delle modalità di utilizzo dell'energia e delle risorse naturali. Nel contempo, l'Europa ha bisogno di un settore digitale che ponga al centro la sostenibilità. Cfr., Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni “*Il Green Deal europeo*”, COM/2019/640 final.

⁴ Secondo la Commissione europea, i dispositivi connessi superano già il numero delle persone sul pianeta, e si prevede che il loro numero salirà a 25 miliardi entro il 2025: un quarto di questi si troverà in Europa. Cfr., Comunicazione congiunta al Parlamento europeo e al Consiglio, “*La strategia dell'UE in materia di cibersicurezza per il decennio digitale*”, JOIN(2020)18 final.

Le nuove tecnologie sono presenti ormai in ogni ambito. Anche il mondo del diritto⁵ e il procedimento penale non è rimasto immune a tale fenomeno⁶: in particolare, nella fase delle indagini preliminari, caratterizzata dal compimento di ogni attività necessaria per le determinazioni inerenti all'esercizio dell'azione penale⁷, si assiste all'impiego di tecnologie investigative che assumono un ruolo di primo ordine nella repressione dei reati; nel processo penale si nota un appannamento della prova testimoniale⁸, basata sulle dichiarazioni rese da persone che hanno conoscenza dei fatti oggetto di prova e che risultano terzi rispetto ad essi⁹, a favore dapprima della c.d. prova scientifica, poi della prova tecnologica¹⁰.

Dunque, sempre più nei processi penali degli Stati democraticamente avanzati si impone con forza l'utilizzo delle nuove tecnologie e con esse della prova informatica, tecnologica e digitale¹¹.

⁵ Cfr., V. FROSINI, *Il diritto nella società tecnologica*, Milano, 1980.

⁶ Sul punto, A. MARANDOLA, *La tutela dell'identità personale (informatica), anche del soggetto coinvolto in un processo penale*, in *Proc. pen. e giust.*, 3, 2017, p. 371, secondo la quale «il processo e i soggetti che ne sono coinvolti subiscono, nell'ambito della nuova era globalizzata, anche un coinvolgimento “tecnologico” e non solo mediatico del fenomeno dello sviluppo tecnologico».

⁷ Cfr. il trittico normativo composto dagli artt. 50, 326 e 358 c.p.p.

⁸ Sui recenti approdi in tema di testimonianza nel processo penale, G. GIOSTRA, *Appunto per una giustizia non solo più efficiente, ma anche più giusta*, in *Politica del diritto*, 4, 2021, p. 609 ss.

⁹ Per uno studio, L. KALB, *La “ricostruzione orale” del fatto tra “efficienza” ed “efficacia” del processo penale*, Torino, 2005, *passim*.

¹⁰ In tal senso, G. SPANGHER, *Introduzione allo studio del processo penale*, Pisa, 2020, p. 127. L'A., preoccupandosi della lesione di possibili diritti fondamentali, ha modo di osservare che «lo sviluppo della scienza, per un verso, e l'evoluzione delle moderne tecniche informatiche, dall'altro, consentono di acquisire informazioni molto penetranti [...]. Si prospettano questioni inedite che se per un verso rifluiscono nella tematica tradizionale della prova, e nelle sue problematiche, per un altro, ampliano il panorama dell'atipicità, ponendo non pochi interrogativi sul rapporto con le regole generali, ma anche con il rischio che l'atipicità costituisca un facile *escamotage* per eludere le garanzie poste a tutela del processo». In merito, anche, A. MARANDOLA, *La tutela dell'identità personale (tra oblio e storicità del fatto)*, in AA.VV., *La vittima del processo. I danni da attività processuale penale* (a cura di G. SPANGHER), Torino, 2017, p. 361, secondo la quale con l'informatizzazione «l'episodio risalente, remoto, in qualsiasi modo concluso, è suscettibile di rivivere e di essere rivissuto. Spesso rivive ed è rivissuto nelle immagini del passato, anche se superate dagli sviluppi successivi».

¹¹ Sul punto, L. LUPÀRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in AA.VV., *Investigazione penale e tecnologia informatica* (a cura di L. LUPÀRIA, G. ZICCARDI) Milano, 2007, p. 128. Secondo l'A. «negli ultimi decenni l'accertamento penale si è lentamente arricchito di inediti contenuti scientifici e di apporti tecnologici di sempre maggiore complessità. Eppure, di fronte a siffatta mutazione della scena processuale, invasa da una congerie di prove tecnico-scientifiche ad elevato grado di specializzazione, poche sono state le voci che hanno saputo preconizzare quello che da lì a poco sarebbe accaduto. Solo oggi, con grave ritardo, iniziamo ad avvertire l'enorme impatto che il proliferare della *scientific evidence* ha sortito sul processo penale, tanto da doverci addirittura interrogare se abbia ancora senso parlare della prova orale in termini di chiave di volta del processo accusatorio, allorché sempre più giudizi paiono fondarsi su evidenze scientifiche formatesi nella prima fase del procedimento e che, veicolate nella scansione dibattimentale, riducono il “contraddittorio per la prova” ad un mero esercizio di dialettica su materiali non facilmente decifrabili e già “preconfezionati” in sede di indagini preliminari». Cfr., anche, G. CANZIO, *Prova scientifica, ricerca della «verità» e decisione giudiziaria nel processo penale*, in *Decisione giudiziaria e verità scientifica*, Quaderni della Rivista trimestrale di diritto e procedura civile, 3, 2005, p. 55; O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005; ID., *In tema di nuova prova scientifica*, in *Dir. pen. Proc.*, 9, 2001, p. 1061; P. TONINI, *Prova scientifica e contraddittorio*, *ivi*, 12, 2003, p. 1459. Per una visione generale sul tema, A. LEIPOLD, *How the pretrial process contributes to wrongful convictions*, in *The American Criminal Law Review*, 4, 2005, p. 1123.

Si passa così dai discorsi che evocano immagini proprie della retorica classica greca e latina¹² alle immagini generate dai mezzi multimediali (sia audio, sia video) dell'era digitale che rendono più vivo il fatto, evocandolo con maggiore chiarezza; da un accertamento processuale affidato alla rievocazione dell'evento attraverso la deposizione testimoniale, con i suoi insiti e insuperabili limiti cognitivi e mnemonici, al «realismo gnoseologico della “verità digitale”»¹³, dall'evidente utilità euristica, appagante alcuni sensi, ma purtroppo impoverendo il giudice di rilevanti elementi percettivi.

¹² Nel *Gorgia* Platone fa definire al filosofo siceliota la retorica come l'arte delle parole, intesa quale capacità di persuadere mediante i discorsi. L'oggetto riguarderebbe il rapporto umano, il costituirsi della vita comune, ossia la vita politica nei tribunali, nella piazza, nel Consiglio. Pertanto, è necessario conoscere la funzione che assumono certe parole rispetto alle altre, certi nessi sintattici rispetto ad altri, certi *tòpoi* (in greco, τόποι) e *figure*, come ad esempio le metafore. Solo applicando correttamente tali conoscenze sarebbe possibile, secondo Gorgia, individuare una soluzione secondo misura, cioè secondo il giusto, inteso nel senso di “ragionevolezza” costruita mediante il discorso. La retorica, dunque, andrebbe alla ricerca del giusto.

¹³ Così, testualmente, F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. e proc. pen.*, 2021, p. 502.

Il processo di digitalizzazione¹⁴ – ben distinto dalla digitalizzazione del processo¹⁵ – può apparire fenomeno recente. In realtà poggia le proprie basi in un contesto temporale

¹⁴ Per processo di digitalizzazione si intende la serie di attività compiute grazie all'evoluzione tecnologica al fine di ottenere un graduale passaggio dalla tecnologia analogica alla tecnologia digitale attraverso l'implementazione di strumenti tecnologici capaci di memorizzare, modificare e recuperare dati, nonché di tecnologie informatiche impiegate nell'ambito delle telecomunicazioni, volte alla trasmissione di segnali mediante un mezzo che collega due terminali.

Altri hanno definito il processo di digitalizzazione come la rappresentazione di ogni dato di realtà tramite codici binari. La definizione è contenuta nel saggio di N. NEGROPONTE, *Being Digital*, New York, pubblicato per la prima volta nel 1995. In esso si spiega che il *bit* è la parte più piccola dell'informazione digitale, così come l'atomo lo è per la materia. Tramite il *bit* si può descrivere il mondo materiale in molte delle sue componenti nelle forme numeriche del codice binario "0" e "1". Similmente anche C. GATTEI, *Tutela dell'opera multimediale su rete telematica: la situazione europea*, in *Dir. Informatica*, 2, 1998, p. 469. Per un profilo storico, M.G. LOSANO, *Scripta volant: la volatilizzazione dei documenti nell'era digitale*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2020, p. 17 ss.

In Italia, negli ultimi anni si è assistito ad una accelerazione del processo di digitalizzazione della giustizia, basato anche sull'uso della posta elettronica certificata (PEC), come stabilito dal Protocollo d'intesa del 26.11.2008 tra il Ministro della Giustizia e il Ministro per la Pubblica Amministrazione e l'innovazione. Tra gli obiettivi programmati in tale sede, è stata individuata anche la digitalizzazione delle comunicazioni e delle notificazioni nel processo civile ed in quello penale, sostituendo il documento digitale al cartaceo così favorendo la riduzione dei costi e dei tempi di notifica ed una maggiore ottimizzazione delle risorse. (Cfr., Cass., Sez. IV, 06-12-2016, n. 51961).

L'impiego di sistemi digitali che consentono la memorizzazione, la modifica, elaborazione e il recupero dei dati prende il nome di *Information Technology* (IT); mentre l'uso delle tecnologie informatiche nell'ambito delle telecomunicazioni è detto *Information and Communication Technology* (ICT). A tal proposito si distingue tra reti di comunicazione elettronica e servizi di comunicazione elettronica. L'art. 2 della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) definisce, ai fini della stessa, reti di comunicazione elettronica «i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa *Internet*), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato», mentre intende per servizi di comunicazione elettronica «i servizi forniti di norma a pagamento consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ma ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 1 della direttiva 98/34/CE non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica». Nell'ordinamento italiano, l'art. 1, d.lgs. 1° agosto 2003, n. 259 (*Codice delle comunicazioni elettroniche*) ha recepito le definizioni contenute nella direttiva, modificandole parzialmente al fine di adattare al contesto nazionale, pur sempre nel rispetto dello spirito di armonizzazione che anima la normativa sovranazionale. L'art. 1, lett. dd), d.lgs. 1° agosto 2003, n. 259 intende per reti di comunicazione elettronica «i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa *Internet*), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato», mentre l'art. 1, lett. gg) d.lgs. 1° agosto 2003, n. 259 definisce servizi di comunicazione elettronica «i servizi, forniti di norma a pagamento, consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, ad esclusione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che

relativamente remoto. Già negli anni '70 del secolo scorso si notò come l'evoluzione della società dava maggior impulso all'economia dei servizi, la quale si contrapponeva lentamente – ma con determinazione – all'economia industriale. L'impatto di essa era dovuto ad un modello sociale che stava dando vita ad un nuovo settore economico basato su un approccio moderno al mondo empirico e fenomenico causato dall'avvento nel contesto mondiale delle nuove tecnologie¹⁶. Era l'inizio dell'era digitale o dell'informazione¹⁷.

esercitano un controllo editoriale su tali contenuti; sono inoltre esclusi i servizi della società dell'informazione di cui all'articolo 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, non consistenti interamente o prevalentemente nella trasmissione di segnali su reti di comunicazione elettronica».

Per una definizione di *Information Techonology* (IT) ed *Information and Communication Technology*, v. S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018, p. 9 ss.

¹⁵ Quando si parla di digitalizzazione del processo ci si riferisce al processo digitale inteso quale adozione estesa e integrata delle tecnologie informatiche nello svolgimento delle funzioni e nell'erogazione dei servizi della giustizia. Il concetto stesso di digitalizzazione del processo farebbe riferimento evidentemente all'innovazione in senso ampio come evoluzione dell'amministrazione della giustizia attivata dalle tecnologie informatiche. Non significa una semplice automazione, ma implica un profondo ripensamento di relazioni, attività e situazioni giuridiche, in cui le tecnologie informatiche non costituiscono il fine ultimo, ma rappresentano lo strumento idoneo a raggiungere gli obiettivi che caratterizzano il processo, ossia il provvedimento finale.

Lo sviluppo telematico della giustizia, in particolare penale, ha ricevuto un forte impulso in occasione della diffusione pandemica del COVID-19. Proprio questo è stato un banco di prova per constatare come alcune tecniche e procedure possono essere lesive del diritto di difesa o di altri diritti fondamentali del processo come l'oralità, l'immediatezza, la concentrazione ed il contraddittorio, sino a coinvolgere il più ampio diritto alla riservatezza. Per un approfondimento, G. SPANGHER, *Covid-19: nel disastro si vede chiaro*, in *Penale diritto e procedura*, 21 aprile 2020, secondo il quale «se indubbiamente alcune modalità informatiche di attività processuali potranno – forse dovranno – essere confermate, come quelle legate all'uso della PEC, alla trasmissione degli atti, alle iniziative processuali, alle notificazioni, molte cautele, se non addirittura, l'oblio, dovrà essere riservato ad alcune modalità di procedimenti a distanza che pregiudicano fortemente il ruolo della difesa. Non si tratta cioè soltanto del perfezionamento delle tecniche, ma proprio del “recupero” della centralità della celebrazione nelle aule dei palazzi di giustizia, da ripristinare da subito, pur nella necessità di assicurare medio tempore il distanziamento sociale». Critica sul punto anche I. CONTI, *Il processo penale al tempo del COVID-19: le udienze a distanza*, in *Penale diritto e procedura*, 18 marzo 2020.

¹⁶ Per una trattazione sui profili sociologici ed economici relativi alla nascita ed allo sviluppo della società dell'informazione, cfr. A. MATTELART, *Storia della società dell'informazione*, Torino, 2002. Nel panorama della letteratura straniera, cfr. E. NEVEU, *Une société de communication?*, Paris, 1994; F. WEBSTER, *Theories of the information society*, London, 1995; M. CASTELLS, *The age of information*, Oxford, 1996; v. anche W.H. DUTTON, *Society on the line*, Oxford, 1999, tradotto in italiano *La società on line. Politica dell'informazione nell'era digitale*, Milano, 1999. Cfr., inoltre, E. SEVERINO, *Il destino della tecnica*, Milano, 1998; E. RESTA, *Il diritto, la libertà, la tecnica*, in *Riv. crit. dir. priv.*, 1, 2001, p. 79.

¹⁷ Il concetto di “era dell'informazione” venne teorizzato per la prima volta nel 1971 da T.C. HELVEY in *Age of Information: An Interdisciplinary Survey of Cybernetics*. La terminologia “rivoluzione informatica” è rinvenibile nelle teorie di D.M. LAMBERTON, il quale nel 1974 scrisse il celebre *Information Revolution*. Per uno studio, J.R. BENIGER, *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard, 1986. Sul concetto di rivoluzione dell'informazione come quarta rivoluzione, L. FLORIDI, *Infosfera: etica e filosofia nell'età dell'informazione*, Torino, 2009; ID., *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Milano, 2017.

Va considerato che è a partire dal 1940 che emergono le “nuove scienze”, il cui tema centrale è l'informazione. Ed invero, la definizione del campo di indagine della teoria dell'informazione risale a C.E. Shannon, mentre quella della cibernetica a N. Wiener nel 1948, epoca in cui l'informazione assume le forme di un'attività economica. Fu in questo periodo che si comprese come l'informazione poteva essere economicamente fruttuosa, per cui cominciarono a sorgere industrie ed istituzioni che occupavano di raccolta, elaborazione, produzione, trasmissione e distribuzione di essa.

Questa vera e propria rivoluzione ha investito ogni sfera della vita, degli interessi delle persone e della collettività; ha coinvolto gli stili di vita e ha scandito nuovi ritmi nella società, modificando il lavoro, l'economia, la produzione, il commercio, la politica, la democrazia¹⁸. E se è vero che, nel quotidiano, ogni vicenda umana è interessata da regole giuridiche, allora nascono, si modificano e si rideterminano nuovi rapporti giuridici¹⁹. Non solo muta il diritto, ma potrebbero svilupparsi nuove branche di esso²⁰.

Siccome facilita la creazione di entità nuove attraverso la combinazione di elementi, opere o dati preesistenti che possono circolare in uno spazio virtuale ubiquitario senza limiti di territorialità²¹, il processo di digitalizzazione ha subito un'accelerazione con lo sviluppo successivo delle tecnologie dell'informazione e della comunicazione. In particolare, la diffusione dei computer e la nascita della rete internet hanno garantito la possibilità di rappresentare virtualmente molte delle cose che siamo abituati ad

Lo studio dei risvolti penalistici dovuti all'impiego delle nuove tecnologie è relativamente recente. La dottrina e la giurisprudenza – anche oltreoceano – hanno cominciato ad occuparsene solo da breve tempo. Per un quadro storico e sistematico, si rinvia a O.S. KERR, *Computer Crime Law*, Thomson West, St. Paul MN, 2018, p. 1-277, ove è possibile rintracciare anche una interessante bibliografia e giurisprudenza americana sul tema. Tradizionalmente, il dibattito dottrinale è stato avviato da D.B. PARKER, *Crime by Computer*, New York, 1976, p. 1-308.

¹⁸ In tal senso, L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 37.

¹⁹ La dottrina ha osservato che ha giuridicità ogni fatto della realtà sociale, anche se semplice ed apparentemente insignificante. «Fatto rilevante è non soltanto quello produttivo di conseguenze giuridiche ben individuabili, ma ogni fatto che, in quanto espressione positiva o negativa (fatto illecito) di regole o di principi presenti nell'ordinamento, abbia una propria significatività secondo il diritto». Cfr. P. PERLINGIERI, *Il diritto civile nella legalità costituzionale, secondo il sistema italo-comunitario delle fonti*, tomo II, Napoli, 2006, p. 600 ss.

Ed invero, si potrebbe affermare che il semplice fatto che Tizio possa accedere alla rete *Internet* e navigare sia giuridicamente rilevante, in quanto manifestazione di valori e principi giuridici che coinvolgono non solo il principio di uguaglianza, ma anche la libertà di informazione, come il diritto a essere informati oltreché a informare, la libertà di comunicazione, la libertà di associazione, la libertà di riunione, la libertà di iniziativa economica privata, e le libertà politiche, tutte declinate alla luce delle nuove tecnologie informatiche.

Sul tema, L. CUOCOLO, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, 2/3, 2012, p. 263 ss.; S. RODOTÀ, *Una Costituzione per Internet?*, in *Politica del diritto*, 2, 2010, p. 337 ss.; ID., *Prefazione*, in AA.VV., *Internet, i nostri diritti* (a cura di A. MASERA, G. SCORZA), Bari, 2016, p. VII ss. Sul punto anche N. LUCCHI, *La legge Création et Internet: le censure del Conseil constitutionnel*, in *Quad. cost.*, 2, 2010, p. 375 ss.

²⁰ La dottrina ha osservato che i nuovi sviluppi scientifici, culturali e politici hanno sviluppato situazioni inedite e imprevedibili che «pongono sempre più l'uomo contemporaneo, in tempi serrati, di fronte a nuove sfide e decisioni, che richiedono risposte non semplici, per le complessità o le novità, che vi sono sottese. Significative indicazioni in tal senso emergono dall'inesplorata potenzialità dello sviluppo tecnologico e dall'evoluzione dei bisogni e delle aspettative legate al mutamento delle dinamiche sociali». Tali dinamiche hanno generato profonde trasformazioni, aprendo «una fase di transizione nella quale si alternano accelerazioni e riflussi, rigetti e spinte evolutive», convergente verso lo stesso prodotto: la legge. In tal senso, G. SPANGHER, *Il difficile governo della complessità*, in *Intelligence Security Investigation*, 20 giugno 2021, disponibile al link: <https://intelligencesecurityinvestigation.it/il-difficile-governo-della-complessita/>.

²¹ Sul punto, G. PASCUZZI, R. CASO, *I diritti sulle opere digitali*, Padova, 2002, p. 13 ss., i quali sostengono che la digitalizzazione rende molto più facile l'attività volta al progresso dell'umanità. Ciò si verifica mettendo insieme dati, informazioni, conoscenze e scoprendo rapporti, relazioni, interazioni, associazioni tra loro. Il prototipo di tale modello è rappresentato dalle opere multimediali. Sui problemi posti dall'opera digitalizzata alle regole tradizionali di diritto, cfr. anche T. DREIER, *Adjustment of Copyright Law to the Requirements of the Information Society*, in *IIC*, 6, 1998; J. STERLING, *Philosophical and Legal Challenges in the Context of Copyright and Digital Technology*, *IIC*, 5, 2000.

immaginare come indissolubilmente legate ad un elemento materiale, attraverso l'uso di un codice binario elaborato mediante strumenti automatici²².

Il fenomeno della digitalizzazione e lo sviluppo delle reti informatiche hanno facilitato la cooperazione transfrontaliera tra Stati membri dell'Unione europea. Tuttavia, lo spazio di libertà, sicurezza e giustizia²³ non è ancora un'area ove le procedure sono pienamente automatizzate e interconnesse tra i suoi Stati membri. Ciò giova alla criminalità organizzata transnazionale che, organizzandosi in tempi più brevi, raggiunge spesso l'obiettivo della circolazione del crimine in modo indisturbato.

Tale consapevolezza ha spinto l'Unione europea a programmare e compiere passi importanti verso un serio processo di digitalizzazione dell'intera area, mediante lo sviluppo non solo di tecnologie e piattaforme informatiche ma anche di norme comuni di armonizzazione che tendono a combattere la criminalità organizzata transfrontaliera sviluppatasi sotto le forme della *cyber*-criminalità.

Ciò nonostante, si constata la difficoltà degli ordinamenti a tenere il passo con lo sviluppo delle nuove tecnologie. La tecnica avanza senza attendere la relativa normazione. Si determinano continui mutamenti nell'ordine tecnologico ed in quello sociale, mentre l'assetto ordinamentale appare sempre in ritardo rispetto alle esigenze di

²² Sul punto, A. GAMBINO, A. STAZI, D. MULA, *Diritto dell'informatica e della comunicazione*, Torino, 2019, p. 3 ss.; M. OREFICE, *I big data. Regole e concorrenza*, in *Politica del diritto*, 4, 2016, p. 698; M. CASTELLS, *La nascita della società in rete*, Milano, 2014, p. 32. Cfr. anche: A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2019, p. 442 ss.

Uno dei modi più comuni attraverso cui generare i dati era la trasposizione degli oggetti della vita reale in formato digitale. Di recente, grazie alla tecnologia, l'essere digitale può esistere fin dall'inizio in quanto tale. Questo è il caso, ad esempio, delle entità non materiali che esistono nella sfera intellettuale degli individui e che possono essere riprodotte con l'uso di un computer sotto forma di contenuti digitali. Cfr., A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche*, cit., p. 442. In tal senso, anche J. SYLVESTRE BERGÉ, S. GRUMBACH, V. ZENO-ZENCOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, 2, 2018, p.149.

²³ Per un approfondimento sul tema, con particolare riferimento alla rilevanza dello spazio di libertà, sicurezza e giustizia v., nello specifico, A. DI STASI, *Tutela multilevel dei diritti fondamentali e costruzione dello spazio europeo di giustizia*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale del titolo VI della Carta* (a cura di A. DI STASI), Napoli, 2019, p. 11 ss. Con particolare riferimento alla cooperazione giudiziaria in materia penale, A. DI STASI, *Spazio europeo di libertà, sicurezza e giustizia e cooperazione giudiziaria in materia penale: il rispetto dei diritti fondamentali e della diversità tra ordinamenti nazionali e tradizioni giuridiche*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. *Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012, p. 3 ss. Inoltre, nell'alluvionale letteratura, si veda G. CAGGIANO, *L'evoluzione dello spazio di libertà, sicurezza e giustizia nella prospettiva di un'Unione basata sul diritto*, in *Studi sull'integrazione europea*, 2, 2007, p. 335 ss.; C. CHEVALLIER-GOVERS, *L'Espace de liberté, de sécurité et de justice (ESLJ)*, in *Revue du droit de l'Union Européenne*, 2, 2018, p. 114 ss.; U. DRAETTA, N. PARISI, D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia dell'Unione europea: principi fondamentali e tutela dei diritti*, Napoli, 2007; M. FLETCHER, E. HERLIN-KARNELL, C. MATERA (eds.), *The European Union as an Area of Freedom, Security and Justice*, London e New York, 2016; A.H. GIBBS, *Thinking constitutionally about the European Union's area of freedom, security and justice*, Thesis – European University Institute, 2009; N. NAVARRO BATISTA, *The development and consolidation of the Area of Freedom, Security and Justice*, in *Revista General de Derecho europeo*, 2017, pp. 389-392; D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia*, Napoli, 2010; L. SALAZAR, *La costruzione di uno spazio penale comune europeo*, in AA.VV., *Lezioni di diritto penale* (a cura di G. GRASSO, R. SICURELLA), Milano, 2007, p. 395 ss.; A.M. STILE, *The Instruments of the Former third pillar in the Lisbon era: towards an Integrated Judicial Control in the Area of Security, Liberty and Justice*, in *New Journal of European Criminal Law*, 4, 2015, p. 482 ss.

regolazione flessibile determinate dalle innovazioni della tecnica che continuamente si innestano nella società 2.0 dell'era digitale²⁴.

La recente insorgenza della pandemia da COVID-19 e la continua interruzione delle interazioni sociali in tutto il mondo hanno esacerbato ulteriormente questi problemi²⁵. Siccome individui, imprese e governi dipendono sempre più dall'uso delle tecnologie informatiche a causa delle restrizioni legate alla pandemia, la criminalità informatica è in continuo aumento. Da qui nasce la necessità di una cooperazione ancora più forte ed efficiente.

2. La metamorfosi della criminalità transnazionale nell'era del digitale: fenomenologia della criminalità informatica organizzata e della criminalità informatica

La smaterializzazione degli enti – intesi nel senso proprio dato da Tommaso D'Aquino – dovuta all'evoluzione digitale ha consentito una modifica delle modalità di accesso ed approccio al crimine. Anche la criminalità evolve trovando nuovi metodi per la consumazione dei reati²⁶. L'assenza di confini definiti e determinati nel tempo e nello spazio ha provocato nella criminalità organizzata un nuovo modo “di pensare”. Per risultare efficace, la lotta ad essa deve essere quanto più veloce possibile. Non sono ammessi ritardi, tentennamenti e proroghe: il rispetto dei tempi contingentati risulta essere fondamentale per colpire efficacemente il crimine.

Ormai è divenuta prassi comune in molte parti del mondo usare i social media, la posta elettronica, i servizi di messaggistica e le applicazioni – le cc.dd. *app* – per comunicare, lavorare, socializzare e ottenere informazioni. Queste ultime, infatti, riescono a circolare con una velocità ed una capacità di diffusione superiore rispetto al passato²⁷. Tali servizi di comunicazione hanno il pregio di interconnettere utenti da una parte all'altra del globo terrestre e di garantire il progresso mondiale, contribuendo notevolmente al benessere economico e sociale di tutta l'Unione europea e della quasi totalità degli Stati presenti nel panorama internazionale.

Grazie al *web* si può entrare in contatto con un numero indecifrabile di persone, enti, associazioni sparsi in ogni parte del pianeta, in tempo reale e, eventualmente, in modo sincronico fra più soggetti, attraverso lo scambio di dati immateriali che si trasformano

²⁴ Cfr., G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2002, p. 20; V.M. SBRESCIA, *Le comunicazioni elettroniche tra tecnologia e regolazione*, in *Riv. it. dir. pubbl. comunit.*, 5, 2011, p. 1207 ss.; M.G. LOSANO, *Dei diritti e dei doveri: anche nella tutela della privacy*, in AA.VV., *La legge italiana sulla privacy. Un bilancio dei primi cinque anni* (a cura di M.G. LOSANO), Roma-Bari, 2001, p. VI. Quest'ultimo evidenzia criticamente che «i tempi cambiano mentre le leggi stanno ferme».

²⁵ Sulle scelte normative e sulle conseguenti misure adottate nel periodo della pandemia, L. KALB, *Emergenza sanitaria e giustizia penale. Un'analisi delle misure incidenti sul sistema processuale penale*, in *Dir. pen. e proc.*, 7, 2020, p. 910 ss. Con specifico riferimento al procedimento cautelare, D. CIMADOMO, *La sospensione dei termini di durata delle misure cautelari personali per emergenza epidemiologica da Covid-19. A proposito di virus...*, in *Dir. pen. e proc.*, 7, 2020, p. 915 ss.; A. MARANDOLA, *Giustizia penale e Covid-19 nella legge n. 70 del 2020*, in *Studium Iuris*, 10, 2020, p. 1170 ss.

²⁶ Sul punto sia consentito il rinvio ad A. GAUDIERI, *Estorsione via chat e gravi indizi di colpevolezza nel procedimento penale*, in *Diritto di internet*, 2, 2019, p. 141.

²⁷ Sul punto, P. CARETTI, A. CARDONE, *Diritto dell'informazione e della comunicazione nell'era della convergenza. Stampa, radiotelevisione, telecomunicazioni, internet, teatro e cinema*, Bologna, 2019, p. 256.

in scritti, suoni, immagini e video²⁸. Non esistono barriere: chi trasmette o riceve potrebbe essere chiunque, in un sistema che appare globale e difficilmente controllabile. *Internet*, infatti, è chiaramente uno straordinario «catalizzatore essenziale della globalizzazione contemporanea»²⁹, vero e proprio motore propulsivo di informazioni circolanti a livello globale.

Tuttavia, può essere utilizzato impropriamente come strumento per commettere o facilitare reati, tra cui gli attentati terroristici. La rivoluzione informatica o cibernetica ha quindi prepotentemente innescato nello scenario globale nuove forme di condotte ritenute illecite, poiché violano o minacciano gravemente diritti ed interessi meritevoli di tutela che coinvolgono persone, gruppi sociali e la collettività³⁰.

La criminalità, infatti, ha trovato terreno fertile e facile accesso ai nuovi strumenti digitali per consumare reati, anche particolarmente gravi, riuscendo a massimizzare i profitti³¹. Proprio i servizi e le *app* sono spesso l'unico posto in cui è possibile rinvenire risultati investigativi utili al fine di individuare gli autori dei reati e ottenere elementi probatori spendibili in giudizio.

In un simile contesto si sviluppano nuove forme di criminalità transnazionale³². Una definizione convincente di criminalità transnazionale può ricavarsi dalla Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale secondo la quale si intende un gruppo strutturato di tre o più persone, esistente per un periodo di tempo che agisce al fine di commettere uno o più gravi crimini o reati stabiliti dalla Convenzione stessa, al fine di ottenere, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale ed acquisisca il carattere della transnazionalità qualora il reato sia:

a) commesso in più di uno Stato;

²⁸ Così, A. SPADARO, *Gli effetti costituzionali della c.d. "globalizzazione". Storia di una "metamorfosi": dalla sovranità dei popoli nazionali alla sovranità dell'opinione pubblica (e della finanza) internazionali*, in *Politica del diritto*, 3, 1998, p. 447. Sul punto, storicamente, v. anche, L. LOMBARDI VALLAURI, *Democraticità dell'informazione giuridica e informatica*, in *Informatica e diritto*, 1975, p. 2 ss.; F.C. AETERTON, *Teledemocracy. Can technology protect democracy?*, Newbury Park, 1987; E. FERRI, G. GIACOBBE, G. TADDEI ELMI, *Informatica e ordinamento giuridico*, Milano, 1988; V. FROSINI, *Informatica, diritto e società*, Milano, 1992; ID., *La criminalità informatica*, in *Il diritto dell'informazione e dell'informatica*, 3, 1997, p. 487 ss.; L.K. GROSSMAN, *The Electronic Republic. Reshaping Democracy in the Information Age*, New York, 1995; P. COSTANZO, *Aspetti problematici del regime giuspubblicistico di Internet*, in *Problemi dell'informazione*, 2, 1996, p. 183 ss.; A.M. GAMBINO, *Gli scambi in rete*, in *Il diritto dell'informazione e dell'informatica*, 2, 1997, p. 423 ss.; G. ZICCARDI, *La libertà di espressione in Internet al vaglio della Corte Suprema degli Stati Uniti*, in *Quad. Cost.*, 1, 1998, p. 123 ss.

²⁹ Così, T.W. GOLDSMITH, *Who Controls the Internet? Illusions of a Borderless World*, New York, 2006, p. 179.

³⁰ In tal senso, L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., p. 37. Sul punto anche S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014.

³¹ In argomento, F. SPIEZIA, *Attacco all'Europa*, Milano, 2020, p. 182.

³² L'espressione criminalità transnazionale viene utilizzata per la prima volta in occasione della *Naples Political Declaration an Global Action Plan against Organized Crime* nei lavori dell'ONU (doc. A/49/748). La dichiarazione è frutto della Conferenza ministeriale sul crimine organizzato tenutasi dal 21 al 23 novembre 1994 a Napoli. Il termine da tale momento in poi comparirà regolarmente nei documenti ufficiali, e segnatamente nei lavori preparatori che confluiranno nella Convenzione di Palermo del 2000, la quale all'art. 32 definisce in modo chiaro il reato di criminalità transnazionale. Per un'ampia trattazione del tema si rimanda a E. ROSI, *Criminalità organizzata transnazionale e sistema penale italiano. La convenzione ONU di Palermo*, Roma, 2007. Per un approfondimento sul rapporto tra criminalità e globalizzazione si veda anche R. SCIARRONE, *Processi di globalizzazione e criminalità organizzata*, in AA.VV., *Potere politico e globalizzazione* (a cura di P. FANTOZZI), Catanzaro, 2004, p. 175 ss.

- b) commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avviene in un altro Stato;
- c) commesso in uno Stato, ma coinvolge un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; o
- d) commesso in uno Stato ma ha effetti sostanziali in un altro Stato³³.

Le prime forme di criminalità organizzata transnazionale non sono di certo recenti: una “criminalità transnazionale” si rinveniva già prima della nascita della Comunità Europea e dell’Unione Europea. Si pensi ad esempio alla criminalità organizzata italo-americana, alla mafia Russa, alla criminalità organizzata colombiana finalizzata principalmente (ma non solo) al traffico di sostanze stupefacenti, o ancora alla mafia cinese, attive in un raggio d’azione sicuramente più ampio rispetto ai confini statuali dove sono sorte ed erano operative a livello globale già da vari decenni prima della nascita dell’Unione Europea.

Le organizzazioni regionali, nate con lo scopo di creare una integrazione economica attraverso l’eliminazione delle restrizioni alla circolazione di persone, beni, servizi e capitali hanno però incentivato lo sviluppo di tali forme di criminalità o comunque hanno spalancato le porte a nuovi traffici e mercati illegali. Di certo, però, non è attribuibile a tali organizzazioni la genesi della criminalità organizzata³⁴.

Con la creazione di uno spazio di libertà, le cui basi sono state gettate dal Consiglio di Tampere del 1999³⁵, si sono sviluppate quattro grandi libertà: libera circolazione di persone, merci, servizi e capitali. Esse si ritrovano sotto l’egida di una garanzia ancora *in fieri* di un elevato livello di protezione dei cittadini, da raggiungere attraverso un delicato bilanciamento tra i principi-valori della libertà, della sicurezza e della giustizia, in potenziale o apparente contrapposizione. Emerge con chiarezza la fondamentale esigenza di garantire ai cittadini europei uno spazio sicuro, ove risulti efficiente la lotta contro la criminalità³⁶.

³³ Sul punto, v. il combinato disposto dell’art. 2, lett. a) e art. 3, par. 2 della Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, adottata dall’Assemblea Generale delle Nazioni Unite con Risoluzione A/RES/55/25 del 15 novembre 2000 ed entrata in vigore il 29 settembre 2003.

³⁴ Si pensi all’istituzione dell’Unione Europea, dell’OEA (organizzazione degli Stati Americani), il NAFTA (accordo di Libero Scambio Nordamericano), il MERCOSUR (Mercato Comune del Sud), l’ASEAN (associazione delle Nazioni dell’Asia Sud-Orientale), l’APEC (Asia-Pacific Economic Cooperation), l’UA (Unione Africana).

³⁵ Sono passati ormai più di venti anni dallo storico Consiglio di Tampere, che ha contribuito a gettare ulteriori e forti basi per uno spazio di libertà, sicurezza e giustizia realmente integrato. Le Conclusioni al Consiglio di Tampere evidenziavano, infatti, l’impegno degli Stati membri nel creare uno spazio europeo di giustizia «nel quale chiunque sia in grado di rivolgersi ai tribunali e alle autorità di tutti gli Stati membri, con la stessa facilità con cui potrebbe farlo nel proprio paese», auspicando, inoltre, una «progressiva riduzione, fino alla definitiva abolizione, delle procedure intermedie per il riconoscimento e per l’esecuzione delle decisioni tra gli Stati membri». Sui lavori del Consiglio di Tampere, sulla sua portata storica, sul suo valore nonché sulla sua importanza, anche nell’attuale assetto ordinamentale dell’Unione europea, v. A. DI STASI, *Il perfezionamento dello spazio europeo di libertà, sicurezza e giustizia: avanzamenti e criticità*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia* (a cura di A. DI STASI), Napoli, 2019, p. 117 ss.; L. SALAZAR, *La costruzione di uno spazio di libertà, sicurezza e giustizia dopo il Consiglio europeo di Tampere*, in *Cass. pen.*, 4, 2000, p. 1114 ss. Le conclusioni del Consiglio europeo di Tampere sono pubblicate in *Cass. pen.*, 1, 2000, p. 307 ss. Per un bilancio dei risultati raggiunti nello spazio di libertà, sicurezza e giustizia a vent’anni dal Consiglio di Tampere, si leggano i contributi in A. DI STASI, L.S. ROSSI, *Lo spazio di libertà sicurezza e giustizia. A vent’anni dal Consiglio europeo di Tampere*, Napoli, 2020, pp. 9-552.

³⁶ In tal senso, A. WEYEMBERGH, *Storia della cooperazione*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 215.

Con lo sviluppo dello spazio di libertà, sicurezza e giustizia e con l'evoluzione dell'Unione europea, alle quattro grandi libertà se ne è affiancata una "quinta e sgradita"³⁷: la libera circolazione della criminalità transnazionale, vera e propria minaccia per la stabilità dell'Unione europea. La necessaria lotta a tale forma di criminalità "a carattere europeo" ha spinto l'Unione europea verso lo sviluppo di nuove forme di cooperazione giudiziaria in materia penale.

Com'è noto, la criminalità transnazionale, soprattutto organizzata, è in continua evoluzione e costantemente alla ricerca di nuovi spazi fecondi in cui infiltrarsi, una criminalità sempre più preparata, colta, e quindi, più difficile da sconfiggere con i classici strumenti a disposizione dei singoli Stati. Operando in un contesto che aborre o comunque elude i confini dei singoli Stati, essa sarebbe imbattibile se non attraverso l'unione e la collaborazione tra Stati.

Se la criminalità transnazionale assume sempre più le forme di una *cyber-criminalità*, per combatterla saranno necessari strumenti sempre più evoluti, al passo con i tempi e che riescano ad essere efficaci ed efficienti nei confronti di attività compiute con tecniche di ultima generazione.

La criminalità informatica³⁸ – così come il terrorismo – è un settore del crimine ritenuto particolarmente grave e caratterizzato da una naturale dimensione transnazionale, capace di sfruttare le restrizioni territoriali dell'azione penale statale o di minare lo Stato di diritto e la democrazia nell'Unione europea. Tale evidenza, rinvenibile all'art. 83, par. 1, TFUE, ha spinto gli Stati membri, quali "padroni dei Trattati" dell'Unione europea, a prescrivere che in tali ambiti è possibile «stabilire norme minime relative alla definizione dei reati e delle sanzioni»³⁹, conferendo in tal modo dei «diritti di supremazia»⁴⁰. Tale esigenza deriva appunto dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni. Non vanno poi dimenticati i possibili ambiti di competenza penale «indiretta»⁴¹ individuabili all'art. 83, par. 2, TFUE⁴².

³⁷ Parla di "quinta e sgradita libertà" riferendosi alla libera circolazione dei criminali e del crimine, J. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 346.

³⁸ Nella dottrina italiana, tale denominazione in luogo di quelle inizialmente ricorrenti di "criminalità elettronica" e di "criminalità da computer" è motivata in L. PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, in *Il Diritto dell'informazione e dell'informatica*, 1985, p. 939 ss., con particolare riferimento alla nota 7. Sul punto v. anche L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, 4, 2011, p. 827 ss.; ID., *Studi di diritto penale dell'informatica*, Verona, 1992. Nell'ordinamento italiano si parla per la prima volta di criminalità informatica nel titolo della l. 23 dicembre 1993, n. 547, che ha introdotto nuove fattispecie di reato nel codice penale ed alcune nuove disposizioni nel codice di procedura penale.

³⁹ In tema, A. IERMANO, *La nozione di pena tra forma e sostanza nel sistema di tutela europeo*, Bari, 2018, *passim*.

⁴⁰ Cfr. Bundesverfassungsgericht, secondo senato, 30 giugno 2009, sul Trattato di Lisbona, par.359

⁴¹ Sulla distinzione tra competenza penale «diretta» o «ausiliaria» dell'Unione europea, rispetto a quella degli Stati, e la competenza «indiretta», cfr. Bundesverfassungsgericht, secondo senato, 30 giugno 2009, sul Trattato di Lisbona. Per un commento alla sentenza, M. BÖSE, *La sentenza della Corte costituzionale tedesca sul Trattato di Lisbona e il suo significato per la europeizzazione del diritto penale*, in *Criminalia*, 2009, p. 267 ss.

⁴² Sull'art. 83, par. 2, TFUE, S. MONTALDO, *La competenza dell'Unione europea ad adottare norme penali ex art. 83, par. 2, TFUE e sue possibili applicazioni*, in *Studi sull'integrazione europea*, 1, 2013, p. 101 ss.

In un villaggio globale⁴³ che da reale si trasforma in virtuale, la criminalità transnazionale trova un nuovo terreno fertile per la consumazione dei reati, complice una globalizzazione non solo dei mercati ma anche delle nuove tecnologie informatiche che consente al crimine di espandersi in una rete globale e fitta, composta anche da rapporti intessuti dal crimine situato fisicamente in zone remote del pianeta⁴⁴.

Il fenomeno della globalizzazione informatica ed economica si presenta quale fatto anche – se non soprattutto – «culturale»⁴⁵. Per questo ci si trova di fronte ad un radicale mutamento di identità della società, che pensa ed agisce con nuovi schemi. Si è sviluppato un nuovo complesso rapporto che coinvolge il mondo del diritto, la tecnologia, le forme di organizzazione della società e i rapporti sociali⁴⁶. La sempre crescente interconnessione di persone, luoghi e oggetti presenta molti benefici, però comporta anche un aumento del rischio di criminalità informatica, soprattutto transnazionale.

Come facilmente intuibile, contestualmente allo sviluppo tecnologico informatico nel settore dell'industria e del commercio, si è avuto un incremento di azioni e di condotte criminose basate sull'utilizzo di sofisticati strumenti telematici e di telecomunicazione⁴⁷.

Tale condizione ha dunque consentito anche la globalizzazione del crimine, con la conseguente espansione di esso non solo oltre i confini nazionali, ma anche oltre i confini fisici, riuscendo a consumare i reati in luoghi virtuali.

In passato, il fenomeno e gli effetti della globalizzazione del crimine vennero analizzati nel “Piano d'azione dell'Unione europea in materia di prevenzione e controllo della criminalità organizzata per l'inizio del nuovo millennio”⁴⁸. In esso, si evidenziò il carattere dinamico dei gruppi criminali, che spesso formano partenariati all'interno ed

⁴³ L'espressione “villaggio globale” è di M. McLuhan, (1964), *Gli strumenti del comunicare*, Milano, ed. 2015. L'ossimoro rimanda al concetto di globalizzazione, e ben riassume come il mondo sia diventato e diventi sempre più piccolo grazie alla velocità delle comunicazioni e alla celerità con cui circolano le informazioni, i beni e i servizi, rendendo tutto più accessibile. Per un approfondimento sul tema e per una analisi sulle conseguenze negative e positive si rinvia a Z. Bauman, *Dentro la globalizzazione. Le conseguenze sulle persone*, Roma-Bari, 1998; J. E. Stiglitz, *La globalizzazione che funziona*, Torino, 2006; ID., *Bancarotta. L'economia globale in caduta libera*, Torino, 2010. Sul tema anche F. Sackwald, *La Mondialisation comme facteur d'intégration régionale*, in *Politique étrangère*, LXII, 2, 1997, p. 257 ss.

⁴⁴ In linea con questo pensiero anche L. Palmieri, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, Milano, 2019, p. 3. A parere dell'A., «La dirompente globalizzazione dei rapporti socio-economici e lo sviluppo delle relazioni umane – anche grazie a strumenti tecnologici ed informatici – hanno consentito un sempre più celere progresso sociale, ma al tempo stesso hanno agevolato gli autori dei più svariati crimini, consentendo loro di estendere la propria attività delinquenziale oltre confine, in tal modo coinvolgendo interessi sia individuali che collettivi riferibili a più ordinamenti nazionali».

⁴⁵ Così, A. Spadaro, *Gli effetti costituzionali della c.d. “globalizzazione”. Storia di una “metamorfosi”: dalla sovranità dei popoli nazionali alla sovranità dell'opinione pubblica (e della finanza) internazionali*, cit., p. 446.

⁴⁶ Sul tema, v. U. Pagallo, *Profili tecnico-informatici e filosofici*, in AA.VV., *Cybercrime* (diretto da A. Cadoppi, S. Canestrari, A. Manna, M. Papa), Milano, 2019, p. 3 ss.; ID., *Il diritto nell'età dell'informazione*, Torino, 2015; S. Rodotà, *Il mondo nella rete*, cit., con specifico riferimento a p. 61 ss.; G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015, pp. 1-252. Sull'argomento, anche, A. Lamberti, *Libertà di informazione e democrazia. Approccio multilevel e questioni attuali*, in AA.VV., *Spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. Di Stasi, L.S. Rossi), Napoli, 2020, p. 163.

⁴⁷ Così, S. Aterno, *Acquisizione e analisi della prova informatica*, in *Dir. pen. e proc.*, *Dossier Processo penale e prova scientifica* (a cura di P. Tonini), 6, 2008, p. 61.

⁴⁸ Il Piano è pubblicato in *G.U.C.E.* n. C124/1 del 3 maggio 2000.

all'esterno del territorio europeo⁴⁹. Con lo sviluppo delle reti internet, tale dinamicità risulta essere maggiormente accentuata.

La difficile individuazione fisica del crimine permette al crimine anche di agire in modo occulto, sfuggendo ai possibili controlli ed alle possibili azioni repressive compiute dal singolo Stato, il quale spesso si trova disarmato, poiché non possiede né strumenti tecnologici per colpire e neutralizzarne la diffusione, né norme adeguate che consentano di agire nel pieno rispetto del principio di legalità.

Si potrebbe parlare di una “zona grigia”, di un *web* che consente di agire con attività spiccatamente delittuose ma in assenza di norme effettive che indichino una soluzione a situazioni spesso *borderline*.

Come l'abbattimento dei confini interni all'Unione europea ha favorito la diffusione e la veloce circolazione del crimine transnazionale, così l'assenza di confini reali all'interno dell'*internet* ha concesso un nuovo spazio di consumazione dei reati.

Sebbene il *web* sia e debba essere uno spazio di libertà, ciò non toglie che esso debba assumere anche i contorni di uno spazio di sicurezza e giustizia, in virtù di un delicato e proficuo equilibrio tra interessi contrapposti. Pertanto, l'Unione europea ha introdotto una serie di iniziative volte a combattere la *cyber-criminalità* transnazionale che dilaga nello spazio virtuale europeo ed extra-europeo. È necessario, però, nello spirito dei Trattati, bilanciare le esigenze repressive e di efficace contrasto della criminalità transnazionale con la tutela dei diritti fondamentali della persona, in quanto la semplificazione e la maggior velocità delle procedure attuate per la lotta alla criminalità transnazionale non possono spingersi sino a pregiudicare l'assetto delle garanzie che ruotano intorno al procedimento penale.

Infatti, la lotta alla criminalità informatica ed alle attività illecite nello spazio virtuale non deve oscurare gli aspetti positivi derivanti da un cyberspazio libero ed aperto, in grado di offrire nuove possibilità per la condivisione di conoscenze e la promozione dell'inclusione politica e sociale a livello mondiale⁵⁰.

Si è sviluppata così una nuova forma di criminalità transnazionale, il cui *locus commissi delicti* appare essere “virtuale”. In virtù di tale astrattezza, l'esigenza di una cooperazione giudiziaria in materia penale è avvertita in campo internazionale come necessaria per le dimensioni e le caratteristiche assunte da tali forme di criminalità.

Nella categoria della criminalità informatica è possibile ricomprendere i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova. Più specificamente, si può operare una classificazione sistematica che include sia i reati informatici in senso stretto ed in senso ampio, sia i reati cibernetici⁵¹.

⁴⁹ Sul punto, F. SPIEZIA, *Coordinamento investigativo delle indagini ed Eurojust*, in AA.VV., «Spazio europeo di giustizia» e *procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012, p. 96 ss.

⁵⁰ Così la risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068(INI)) (2018/C 346/04), in *G.U.U.E.* C 346 del 27 settembre 2018.

⁵¹ Per reato informatico in senso stretto si intende una fattispecie che presenta almeno un elemento che richiama espressamente ed univocamente le *Information and Communication Technology* (ICT) nella descrizione delle modalità di condotta, ovvero dei mezzi, degli oggetti, dell'evento, o di altre condizioni del reato. L'elemento deve essere integrato ai fini della consumazione della fattispecie stessa o nella forma base o nella forma circostanziata; sono reati informatici in senso ampio quelli che possono realizzarsi anche attraverso l'utilizzo di strumenti informatici o oggetti informatici, ovvero con modalità di condotta od effetti che coinvolgono le ICT; i reati cibernetici si caratterizzano per il *locus* in cui si commettono o si possono commettere, ossia in rete ovvero nel *web – rectius*, nel *Cyberspace* – in quanto la fattispecie incriminatrice contiene un elemento essenziale o una circostanza che espressamente richiama la rete (reato cibernetico in

La lotta alla “criminalità informatica” col tempo è assunta ad ambito strategico d'intervento nel sistema *multilevel*, attraverso la creazione di strumenti di diritto penale sostanziale e processuale nonché di tipo preventivo, amministrativo e di polizia, al fine di porre basi giuridiche comuni che vadano verso la creazione di una disciplina omogenea e verso il rafforzamento della cooperazione di polizia e giudiziaria internazionale.

Ed invero, già con la Convenzione del Consiglio d'Europa sulla criminalità informatica⁵², gli Stati membri del Consiglio d'Europa e gli altri Stati firmatari ritennero fosse necessaria una crescente, veloce e ben funzionante cooperazione internazionale in campo penale per una efficace lotta alla criminalità informatica.

Nell'area dell'Unione europea, risalto va dato alla relazione IOCTA 2016⁵³, la quale ha evidenziato che la criminalità informatica è in aumento per intensità, complessità ed ampiezza. In alcuni Paesi membri dell'UE la criminalità informatica denunciata supera i reati tradizionali ed è in forte estensione ad altre sfere della criminalità quali la tratta di esseri umani. Analogamente, anche l'uso di strumenti di crittografia e anonimato a scopi criminali è in aumento e gli attacchi di tipo *ransomware* superano le minacce legate ai

senso stretto), ovvero «prevede elementi di tipizzazione del fatto di reato che solo implicitamente o in via ermeneutica sono compatibili con la concreta realizzazione nel *Cyberspace* (reati cibernetici in senso ampio)». Per un approfondimento, L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., p. 75 ss. Sul punto, v. anche, S.W. BENNER, *Defining Cybercrime: a Review of Federal and State Law*, in R.D. CLIFFORD (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 3rd ed., Raleigh, 2011, pp. 15–104; V. DESTITO, voce *Reati informatici*, in *Dig. disc. pen.*, Agg. V, Torino, 2010, p. 739 ss.; R. FLOR, *Lotta alla “criminalità informatica” e tutela di “tradizionali” e “nuovi” diritti fondamentali nell’era di Internet*, in *Diritto penale contemporaneo*, 20 settembre 2012, disponibile all'indirizzo <https://archivioldpc.dirittopenaleuomo.org/upload/1348049846flor%20corretto.pdf>; P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997; L. LUPÀRIA, *Computer crimes e procedimento penale*, in AA.VV., *Trattato di procedura penale* (a cura di G. GARUTI), Torino, 7, I, 2011, p. 368 ss.; C. MAIOLI, *Dar voce alle prove: elementi di Informatica Forense*, in AA.VV., *Crimine virtuale, minaccia reale. Ict Security: politiche e strumenti di prevenzione*, (a cura di P. POZZI), Milano, 2004, p. 68 ss.; P. PERRI, voce *Computer forensics (indagini informatiche)*, in *Dig. disc. pen.*, Agg. VI, Torino, 2011, p. 100 ss.; G. PICA, voce *Reati informatici e telematici*, in *Dig. disc. pen.*, Agg. I, Torino, 2000, p. 521 ss.; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet* (a cura di L. PICOTTI), Padova, 2004, p. 21 ss. Tuttavia, l'Unione europea propone una suddivisione alternativa. Il reato cibernetico si riferirebbe comunemente a un'ampia gamma di attività criminali diverse in cui i sistemi informativi e i sistemi informatici costituiscono l'arma primaria o il bersaglio primario. Il reato cibernetico – altrimenti detto cibercrimine – comprenderebbe sia reati tradizionali (ad es. frode, contraffazione o furto di identità), reati connessi ai contenuti (ad es. distribuzione in linea di materiale pedopornografico o incitamento all'odio razziale) e reati peculiari ai sistemi informatici e ai sistemi informativi (ad es. attacchi contro i sistemi informativi, rifiuto di servizi o software maligni). Cfr., Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Strategia dell'Unione europea per la cibersecurity: un ciberspazio aperto e sicuro*, JOIN(2013) 1 final.

⁵² Per un approfondimento sulla Convenzione, v. *infra*, Cap. 3.

⁵³ V., più diffusamente, EUROPEAN POLICE OFFICE (EUROPOL), *The Internet Organised Crime Threat Assessment (IOCTA) 2016*, The Hague, 2016, disponibile al link: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016>.

*malware*⁵⁴ tradizionali quali i *trojan*. La relazione SOCTA 2017⁵⁵, inoltre, ha identificato il crimine informatico come una delle dieci priorità nella lotta alla criminalità transnazionale organizzata e grave. Infatti, negli ultimi periodi gli *hacker* si concentrano su obiettivi più redditizi, riuscendo ad infliggere maggiori danni economici⁵⁶. Sono necessari sforzi continui per creare una sinergia tra la rete, il settore della sicurezza informatica, le forze dell'ordine e le autorità giudiziarie che si occupano di *cyber law*, al fine di migliorare la resilienza cibernetica globale e la sicurezza informatica.

Così tratteggiata, risulta palese come la criminalità transfrontaliera informatica sia un fenomeno in forte crescita negli Stati membri. Essa rappresenta una chiara minaccia per lo Stato di diritto nel cyberspazio e mette a repentaglio la stabilità delle società democratiche. Ciò perché provoca spesso notevoli danni socio-economici e lede i diritti fondamentali delle persone⁵⁷.

L'ambito di operatività di questa forma di criminalità è assai vasto perché, in ragione della pervasività con cui gli strumenti informatici hanno conquistato tutti gli spazi della vita quotidiana, ormai è possibile che ogni fatto costituente reato si caratterizzi di aspetti informatici rilevanti.

La straordinaria velocità con cui il progresso tecnologico sta modificando ogni aspetto della vita economica e sociale, pubblica e privata, è all'origine del continuo inseguimento del diritto, volto a regolare ogni fenomeno correlato alle caratteristiche stesse dell'informatica e della telematica, che risultano giuridicamente rilevanti. Le nuove tecnologie stanno modificando le condotte individuali e collettive, ed hanno coinvolto ogni forma di attività e di relazione tra singoli, gruppi sociali, reti, enti ed imprese, fino alle conformazioni sociali illecite e criminose⁵⁸.

Purtroppo, ritardi e difficoltà delle risposte giuridico-penali alle nuove minacce manifestatesi in questo settore sono fisiologiche, poiché i necessari processi di adeguamento delle legislazioni nazionali allo sviluppo ed all'applicazione delle nuove tecnologie non consentono di essere perfettamente al passo con i tempi, complice anche una ragionevole durata dell'*iter* di formazione delle norme, ossequioso dei preminenti principi di democrazia e dello Stato di diritto.

⁵⁴ La facile reperibilità ed il semplice utilizzo di questi tipi di *software* per scopi illeciti è causa di un continuo aumento del numero dei cd. *cyber criminals*, con il serio rischio di una criminalità cibernetica di massa, difficilmente contrastabile, dovuta soprattutto al suo carattere transnazionale. In tal senso, I. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv. it. dir. e proc. pen.*, 2, 2017, p. 747 ss.

⁵⁵ EUROPEAN POLICE OFFICE (EUROPOL), *European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017*, The Hague, 2017, disponibile al link: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017>.

⁵⁶ Come, ad esempio, *trojan* bancari o attacchi contro i sistemi di controllo industriali e le reti mirati a distruggere infrastrutture cruciali e strutture economiche, nonché destabilizzare le società. Sul punto, EUROPEAN POLICE OFFICE (EUROPOL), *The Internet Organised Crime Threat Assessment (IOCTA) 2019*, The Hague, 2019, disponibile al link: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019>. La relazione evidenzia che il *phishing* e gli RDP vulnerabili sono i principali vettori di infezione da *malware*; mentre i dati restano un obiettivo chiave del crimine informatico perché ritenuta merce su cui speculare. Negli ultimi periodi si sta sviluppando anche lo *smishing*, una variante del più famoso *phishing*. Si tratta di un tipo di truffa su internet consumata con una condotta criminale volta ad aggirare la vittima fingendosi un ente affidabile e convincendola a cedere dati personali e finanziari, nonché credenziali o altri codici di accesso.

⁵⁷ Cfr. la risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica (2017/2068(INI)) (2018/C 346/04), in *G.U.U.E.* C 346 del 27 settembre 2018.

⁵⁸ Sul punto, L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, cit., p. 829.

Un ulteriore elemento di criticità è ravvisabile nella necessità di rendere palesi avanti al giudice – chiamato ad accertare la legalità della formazione della prova, l'integrità e la veridicità del suo contenuto – le funzionalità e le caratteristiche tecniche dei dispositivi elettronici utilizzati nelle indagini. Ciò, incontra la resistenza delle case costruttrici, interessate alla tutela del loro *know how*, e finisce per rivelare caratteristiche utili alla criminalità, la quale può sviluppare nuovi strumenti di elusione. Infatti, spesso le successive indagini fatte con i medesimi strumenti non più segreti rischiano di non essere efficienti perché la criminalità informatica ha già creato nuovi *software* in grado di nascondere le proprie tracce agli occhi degli investigatori⁵⁹.

Da qui deriva una obsolescenza forzata delle tecniche di acquisizione ed estrazione della prova e la conseguente corsa a nuovi e più sofisticati strumenti nella lotta alla criminalità informatica organizzata che spesso vede quest'ultima vincente poiché capace di investire nel settore ingenti risorse economiche.

Va però considerato che gli interventi legislativi sono sollecitati sempre più spesso non solo dalle fonti internazionali e sovranazionali, ma anche dalla dottrina e dalla giurisprudenza, che evidenziano costantemente la necessità di un adeguamento normativo volto ad eliminare le lacune emergenti⁶⁰.

La difficoltà di accesso alle prove elettroniche – *rectius*, informazioni elettroniche – e la conseguente difficoltà nell'ottenerle e farle ammettere in tribunale, il più delle volte collegate alle complesse procedure e sfide giurisdizionali connesse al carattere transfrontaliero della criminalità informatica, è una delle cause della notevole quantità di crimini informatici non perseguiti o impuniti.

La cooperazione e lo scambio di informazioni tra le autorità giudiziarie e di polizia ed esperti in materia di criminalità informatica risultano essenziali per lo svolgimento di indagini efficaci nel cyberspazio e per l'ottenimento delle informazioni elettroniche, poiché rappresentano un metodo efficace per contrastare la criminalità informatica – quasi ontologicamente dal carattere transnazionale – e le minacce comuni alla cibersicurezza cui deve far fronte l'Unione europea.

Pertanto, l'Unione europea, da sempre sensibile al tema, sta sviluppando nuovi strumenti di cooperazione giudiziaria in materia penale basate sul principio del mutuo riconoscimento, che vadano nella direzione della celerità della formazione della prova informatica, nel pieno rispetto dei diritti fondamentali della persona. Infatti, la lotta alla criminalità informatica deve rispettare lo stesso livello di garanzie assicurato ai diritti fondamentali tutelati nella lotta alle altre sfere della criminalità, ponendo però particolare attenzione alla protezione dei dati e alla libertà di espressione.

Infatti, la nuova agenda strategica 2019-2024 adottata dal Consiglio europeo il 20 giugno 2019 dà rilevanza allo sviluppo ed all'intensificazione della lotta al terrorismo e alla criminalità transfrontaliera, attraverso: il miglioramento della cooperazione; la condivisione di informazioni; la creazione di strumenti comuni. Ciò perché è necessario proteggere la società europea dalle attività informatiche dolose, dalle minacce ibride e dalla disinformazione provenienti da attori statali e non statali ostili. Per affrontare tali minacce è necessario un approccio globale che veda un rafforzamento in termini di cooperazione, coordinamento, risorse e capacità tecnologiche.

Intanto, nonostante negli ultimi anni la stretta cooperazione tra il Parlamento europeo, il Consiglio, gli Stati membri e la Commissione abbia consentito all'UE di compiere

⁵⁹ In tal senso, C. ASARO, *Sul cammina tracciato da Evidence*, in *Inf. e dir.*, 2, 2016, p. 141.

⁶⁰ Cfr., U. SIEBER, *The International Handbook on Computer Crime*, Portsmouth, 1986; ID., (ed.), *Information Technology Crime*, Köln, 1994.

notevoli progressi nel lavoro congiunto per realizzare un'autentica ed efficace Unione della sicurezza, la Commissione ha sovente invitato il Parlamento europeo e il Consiglio ad adottare le misure necessarie per raggiungere rapidamente un accordo sulle proposte legislative per contrastare la propaganda terroristica e la radicalizzazione online, nonché a rafforzare la cibersecurity, facilitare l'accesso alle prove elettroniche e completare il lavoro su sistemi di informazione più solidi e intelligenti per la sicurezza, le frontiere e la gestione della migrazione, al fine di consolidare la sicurezza di tutti i cittadini⁶¹.

2.1. (Segue). *Il cyber terrorismo*

La diffusione di internet al largo pubblico avvenuta negli ultimi decenni del secolo scorso ha contribuito definitivamente a far assumere una dimensione globale alle reti di comunicazione. Il fenomeno è risultato così rilevante da spingere larga parte dei protagonisti dello scenario internazionale ad interessarsi al tema⁶², nell'intento di regolarne la fruizione e di prevedere norme precettive che fungano da deterrente per la criminalità transnazionale.

È ormai evidente anche ad un occhio non esperto l'impossibile sottrazione di *internet* a regole e norme. L'idea di un *web* quale luogo in cui fiorisce l'anarchia e la totale libertà è indubbiamente utopistica: non può di fatto sottrarsi al diritto dal momento in cui in esso vi siano fatti giuridicamente rilevanti giacché coinvolgono valori e principi⁶³.

Il mondo è cambiato e continua a cambiare. Tanti sono stati gli eventi che hanno contribuito a delineare le caratteristiche della nuova società dell'era digitale a partire dall'attacco al World Trade Center dell'11 settembre 2001⁶⁴. Il nuovo volto del terrorismo internazionale, però, ha subito una rapida evoluzione, sempre più evidente con il succedersi dei drammatici eventi di simile matrice verificatisi in Francia, Regno Unito, Belgio, Spagna, Turchia e Austria, solo per citarne alcuni.

Con la comparsa sulla scena internazionale di forme di terrorismo transnazionale organizzato, i cui tratti salienti spesso si ravvisano nel fondamentalismo "islamico" o "jihadista"⁶⁵, il mondo ha compreso l'importanza della creazione di norme comuni volte

⁶¹ Cfr. le conclusioni alla comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio "Diciannovesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza", COM(2019) 353 final.

⁶² In pochi anni, oltre ai legislatori di quasi tutti gli Stati occidentali, i più autorevoli organismi internazionali si sono impegnati nella lotta alla criminalità nel *cyberspace*. Tra questi si ricordano l'OCSE, il Consiglio d'Europa, l'Unione europea, il WTO, l'ONMPI, il G8, le Nazioni Unite. Cfr. L. PICOTTI, *Le "Raccomandazioni" del XV Congresso Internazionale di Diritto penale in tema di criminalità informatica*, in *Riv. trim. dir. pen. econ.*, 1995, p. 1279 ss.

⁶³ Per un'ampia esposizione del tema, G. ZICCARDI, *Hacker. Il richiamo della libertà*, Milano, 2011.

⁶⁴ Sulle misure antiterrorismo e sul controllo giudiziario nel contesto internazionale a seguito degli attacchi dell'11 settembre 2001, con particolare riferimento al caso " Hamas e LTTE", G. HARPAZ, *Common Foreign and Security Policy, counter-terrorism measures and judicial review: Hamas and LTTE*, in *Common Market Law Review*, 6, 2018, pp. 1917-1940. Nella giurisprudenza, Corte di giustizia, Grande Camera, sentenza del 26 luglio 2017, *Council of the European Union v. Hamas*, Causa C-79/15 P, EU:C:2017:584; Corte di giustizia, Grande Camera, sentenza del 26 luglio 2017, *Council v. Liberation Tigers of Tamil Eelam ("LTTE")*, Causa C-599/14 P, EU:C:2017:583.

⁶⁵ Sempre più spesso con l'espressione "terrorismo internazionale" si fa riferimento al jihadismo o fondamentalismo "islamico", contraddistinto da una dimensione marcatamente transnazionale. Secondo parte della dottrina, l'aggettivo "jihadista" non dovrebbe essere utilizzato per qualificare tale tipologia di terrorismo, poiché il termine "jihad" non alluderebbe in sé alla "guerra santa" condotta dallo Stato islamico e dai suoi affiliati bensì, letteralmente, allo «slancio per raggiungere un dato obiettivo e [...] allo sforzo spirituale del singolo individuo per migliorare sé stesso». Infatti, con il termine *jihad* si fa riferimento al

a contrastare la diffusione del fenomeno⁶⁶. Il metodo adottato da questa nuova forma di lotta terroristica – che molti potrebbero pensare erroneamente sia solo nei confronti dell’Occidente – si è caratterizzata per: la diffusione del terrore tra la popolazione civile attraverso attacchi a sorpresa con modalità spesso di facile esecuzione; l’opera di proselitismo e di adescamento di persone al fine di istigarle a commettere atti terroristici; l’addestramento e la fornitura di istruzioni sulla preparazione o sull’uso di armi, materiali esplosivi o qualsiasi altro oggetto e/o tecnica funzionali all’esecuzione di attività di matrice terroristica; diffusione di informazioni finalizzate all’organizzazione degli attacchi terroristici.

Questo è stato, di fatto, lo schema utilizzato dalle forze armate dell’ISIS-ISIL – l’*Islamic State of Iraq and the Levant* –, da *Al-Qaeda* e dai *foreign terrorist fighters*⁶⁷, i

dovere dei musulmani di osservare e diffondere la fede islamica. Tale fenomeno deve essere tenuto distinto dalla “*violent jihad*”. Sul punto, S. MORETTI, voce *Guerra santa*, in *Treccani online*, disponibile al link: [http://www.treccani.it/enciclopedia/guerra-santa_\(Enciclopedia-dei-ragazzi\)/](http://www.treccani.it/enciclopedia/guerra-santa_(Enciclopedia-dei-ragazzi)/). Sul tema anche F. ROSSI, *Il processo multifattoriale di radicalizzazione al fondamentalismo “jihadista”*, in *Sistema penale*, 6, 2020, p. 305; C. DEL PRADO HIGUERA, E. SÁNCHEZ DE ROJAS DÍAZ, *Terrorismo islamista: El caso de Al Gama’a al Islamiya*, Valencia, 2018, pp. 91 ss. (in particolare p. 92); N. SANZ MULAS, *Las sociedades paralelas como cantera del yihadismo*, in *El terrorismo en la actualidad: un nuevo enfoque político criminal*, dir. da A.I. PÉREZ CEPEDA, coord. da M. RUIZ ARIAS, Valencia, 2018, pp. 252 ss.; A. SPERINI, *I Modelli Sistemici del jihadismo: aspetti evolutivi in chiave anti-sistema*, in AA.VV., *Comprendere il terrorismo. Spunti interpretativi di analisi e metodologie di contrasto del fenomeno* (a cura di R. RAZZANTE), Pisa, 2019, p. 83.

⁶⁶ Su un nuovo approccio per la lotta al terrorismo internazionale, M. NINO, *Le prospettive della lotta al terrorismo internazionale dopo la Conferenza di Revisione dello Statuto della Corte Penale Internazionale*, in AA.VV., *Globalizzazione e pluralità delle fonti giuridiche: un duplice approccio*. Liber Discipulorum *A Dual Approach to Globalization and Legal Pluralism* (a cura di G. ZICCARDI CAPALDO), Napoli, 2012, p. 169 ss.; ID., *Il rapporto tra la lotta al terrorismo e tutela dei diritti fondamentali nell’esperienza giuridica statunitense*, in AA.VV., *Scritti in memoria di Fulvio Fenucci* (a cura di A. BARBERA, A. LOIODICE, M. SCUDIERO, P. STANZIONE), Soveria Mannelli, 2010, p. 485 ss.

⁶⁷ Con l’espressione *foreign terrorist fighters* si fa riferimento ad un nuovo concetto giuridico non ancora definito in modo chiaro. La terminologia è spesso utilizzata per indicare soggetti di nazionalità straniera che prendono parte a conflitti di ogni tipo. I *foreign fighters* possono essere coinvolti in forme diverse all’interno dei conflitti armati poiché questi possono essere semplici mercenari alla ricerca di guadagni personali ovvero combattenti politici per la libertà — come, ad esempio, le brigate internazionali che hanno combattuto contro Franco durante la guerra civile spagnola degli anni ‘30 — oppure combattenti religiosi spinti dal desiderio di creare un Califfato o partecipare alla *jihad*. Solo di recente si sono verificati episodi tali da ricondurre la loro figura anche a ipotesi di terrorismo. In tal caso, si parla di *foreign terrorist fighters* quando consumano reati di matrice terroristica. Il paragrafo 8 della risoluzione n. 2178, approvata all’unanimità dal Consiglio di Sicurezza il 24 settembre 2014 nel quadro del capitolo VII della Carta ONU ha definito i *foreign terrorist fighters* «combattenti che viaggiano verso uno Stato diverso da quello di residenza o di cittadinanza con il fine di commettere, pianificare o preparare attacchi terroristici o di parteciparvi, oppure al fine di fornire o ricevere un addestramento per finalità di terrorismo, anche all’interno di un conflitto armato». Infatti, l’art 6, lett. a) della risoluzione n. 2178 [S/RES/2178(2014)] prevede espressamente un obbligo di incriminazione di essi, per arginare il fenomeno del *blowback*, ossia dell’addestramento di combattenti in Stati stranieri al fine di commettere successivamente attacchi terroristici in Europa. Sul tema, J.A.E. VERVAELE, *Foreign (terrorist) fighters: combattenti, terroristi o solo nemici?*, in *Riv. it. dir. e proc. pen.*, 4, 2018, p. 1875 ss. Sull’argomento, anche, A. ALÌ, *La risposta della Comunità internazionale al fenomeno dei Foreign Terrorist Fighters*, in *La Comunità int.*, 2, 2015, p. 181-201; A. CASSESE, *The Multifaceted Criminal Notion of Terrorism in International Law*, in *Journal of International Criminal Justice*, 5, 2006, p. 933 ss.; A. DE GUTTRY, F. CAPONE, C. PAULUSSEN (eds.), *Foreign Fighters under International Law and Beyond*, The Hague, 2016; M. ENGELHARDT, *Heiliger Krieg, heiliger Profit. Afrika als neues Schlachtfeld des internationalen Terrorismus*, Berlin, 2014; R. HEINSCH, *Foreign Fighters and International Criminal Law*, in A. DE GUTTRY, F. CAPONE, C. PAULUSSEN (eds.), *Foreign Fighters under International Law and Beyond*, cit., p. 161 ss.; L. MARINI, *Foreign terrorist fighters: verso la revisione della risoluzione 2178 (2014)*, in *penalecontemporaneo.it*, 20 dicembre 2017,

quali si scambiavano costantemente informazioni attraverso i dispositivi informatici, navigando spesso indisturbati sul *web*⁶⁸. Modalità simili sono adottate anche dai *lone wolves*⁶⁹, i quali utilizzano il *web* quale canale di diffusione delle informazioni e come strumento per l'addestramento e per la ricerca di mezzi, strumenti e nuove modalità di attacco.

Questi ed altri gruppi armati di stessa matrice utilizzano i mezzi digitali, quali cyberattacchi e sabotaggi alla sicurezza informatica, come strumenti militari strategicamente efficaci per la realizzazione delle loro finalità. Infatti, con il sostegno delle nuove tecnologie informatiche, essi riescono velocemente e con facilità a delocalizzare le loro attività nel territorio delle forze alleate con il loro nemico. Al contempo, adescano, addestrano ed utilizzano i cittadini di queste ultime per sferrare attacchi violenti nei territori di quelle stesse forze alleate e/o se ne avvalgono in qualità di combattenti stranieri nella zona di conflitto. Ciò porta a ritenere che il nesso tra conflitto armato e condotta mantenuta dalle forze armate può essere molto più facilmente delocalizzato grazie all'utilizzo delle tecnologie informatiche rispetto al passato⁷⁰.

Organizzazioni come l'ISIS hanno fatto dell'internazionalizzazione, globalizzazione e digitalizzazione della loro "Guerra santa" un proprio marchio di fabbrica, tanto da poter

disponibile al link: <https://archiviopcd.dirittopenaleuomo.org/d/5760-foreign-terrorist-fighters-verso-la-revisione-della-risoluzione-2178-2014>; ID., *L'evoluzione della disciplina internazionale in materia di terrorismo: qualche spunto recente fra Onu ed Europa*, in *Questione giustizia*, 2, 2017, p. 112 ss.; E. SOMMARIO, *The Status of Foreign Fighters under International Humanitarian Law*, in A. DE GUTTRY, F. CAPONE, C. PAULUSSEN (eds.), *Foreign Fighters under International Law and Beyond*, cit., p. 141 ss. Per un commento critico alla risoluzione, M. SOSSAI, *Foreign Terrorist Fighters: una nozione ai confini del diritto internazionale*, in *federalismi.it*, 25 settembre 2015.

⁶⁸ Il terrorismo è un fenomeno in continua evoluzione. L'UE e i suoi Stati membri devono adattarsi di conseguenza. Nonostante la liberazione dei territori in Siria e Iraq dal controllo di Da'esh, la minaccia rappresentata da Da'esh e Al Qaeda e dai loro affiliati resta elevata. È pertanto necessaria la risoluta mobilitazione della comunità internazionale. Da'esh e Al Qaeda, tentando varie strategie, vogliono mantenere la loro influenza, espandere le loro attività e diffondere la loro ideologia islamista estremista e violenta a livello mondiale in diverse forme, attraverso cellule locali e regionali in tutto il mondo. A tal fine si affidano sempre più alle piattaforme online, divenute ancora più essenziali per diffondere la propaganda terroristica, per ispirare, guidare e dirigere attentati e per promuovere la radicalizzazione che porta all'estremismo violento e al terrorismo. Pertanto, poiché l'impatto della pandemia di Covid-19 rappresenta una sfida senza precedenti con effetti di ampia portata che si manifesteranno appieno solo nel lungo periodo, occorre compiere uno sforzo specifico per valutare la sua potenziale influenza sulle attività terroristiche, nonché sulla prevenzione e sulla lotta contro il terrorismo, e per individuare eventuali azioni mirate dell'UE. Cfr., Conclusioni del Consiglio sull'azione esterna dell'UE per la prevenzione e la lotta contro il terrorismo e l'estremismo violento del 15 giugno 2020, 8868/20, le quali si basano sulle conclusioni del Consiglio sull'azione esterna relativa alla lotta al terrorismo del 9 febbraio 2015 e del 19 giugno 2017, e sono ad esse complementari. Insieme, le tre conclusioni costituiscono le pietre angolari del futuro impegno dell'UE, in linea con la strategia antiterrorismo dell'UE del 2005, con l'Agenda europea sulla sicurezza e con la strategia globale dell'UE del 2016, in cui si rammenta che la sicurezza al nostro interno dipende dalla pace al di là delle frontiere dell'UE.

⁶⁹ I "lupi solitari" sono «soggetti (spesso immigrati di seconda o terza generazione) convertitisi a titolo individuale alla causa fondamentalistica, e disposti ad immolare la propria vita nel compimento di azioni terroristiche per così dire "in proprio", eventualmente avvalendosi delle informazioni sulle modalità di realizzazione di ordigni micidiali reperibili in internet, ovvero mettendo a frutto l'addestramento ricevuto o l'esperienza di combattimento maturata nel corso di viaggi in zone interessate da conflitti armati». Così, F. VIGANÒ, *Minaccia dei "lupi solitari" e risposta dell'ordinamento: alla ricerca di un delicato equilibrio tra diritto penale, misure di prevenzione e tutela dei diritti fondamentali della persona*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo* (a cura di R. KOSTORIS, F. VIGANÒ), Torino, 2015, p. IX.

⁷⁰ In tal senso, J.A.E. VERVAELE, *Foreign (terrorist) fighters: combattenti, terroristi o solo nemici?*, cit., p. 1875 ss.

parlare in tali casi di *Cyberjihad*. Questa, infatti, rappresenterebbe una delle forme in cui si manifesta il *cyber-terrorismo*⁷¹.

Pochi giorni prima dell'attentato a Parigi del 13 novembre 2015⁷² – passato alla storia come l'*attacco al Bataclan* – il ministro degli Interni Belga, Jan Jambon, ha affermato che la *console* per videogiochi *Playstation 4* era diventata strumento di comunicazione tra terroristi, i cui messaggi sono estremamente difficili da captare, riconoscendo che intercettare queste forme di comunicazione «è ancora più complicato che per WhatsApp». Ciò aveva innescato un fervente dibattito politico in Europa ed in Italia, che coinvolgeva il diritto alla riservatezza, la sicurezza e la possibilità di intercettare tali comunicazioni in funzione preventiva e/o repressiva⁷³.

L'osservazione appare acuta, condivisibile e meritevole di approfondimento. Sicuramente il problema non coinvolge solo le *console* da videogioco *Playstation 4*, ma qualsiasi altro dispositivo, anche non simile, in grado di connettersi alla rete e trasmettere messaggi, o qualsiasi altro *hardware* o *software* capace di far comunicare o conversare due persone che utilizzano due dispositivi diversi, in luoghi diversi.

Secondo alcuni studi, i videogiochi sono diventati un mezzo valido e sempre più impiegato nella propaganda digitale ciberterroristica. Il ruolo assunto dai videogiochi in questo contesto è diventato con il tempo così rilevante da aver spinto la dottrina a parlare di “gamificazione della *cyber jihad*”, intendendo con essa l'uso di videogiochi come vettori della campagna di adescamento ed addestramento di possibili *cyber-partisans*⁷⁴.

Il successo di queste modalità è evidentemente dovuto al fascino che i videogiochi emanano, soprattutto tra i più giovani, essendo questi ultimi soggetti maggiormente esposti a vulnerabilità.

⁷¹ A tal proposito, F. SPIEZIA, *Attacco all'Europa*, cit., p. 182, secondo il quale «l'utilizzo di siti web, di social network o di forum e piattaforme online per alimentare il credo jihadista ha portato all'avvento di una nuova era, quella del terrorismo digitale di massa, in cui i gruppi terroristici vedono nel web l'opportunità per mantenere il controllo e la resilienza, anche quando incontrano ostacoli nella realizzazione del progetto di costruzione di uno Stato territoriale». Sul fenomeno del terrorismo internazionale nel contesto di internet, v., inoltre, P. CIRILLO, *Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di Internet*, in *Dir. pen. cont.*, 2, 2019, p. 81 ss.

⁷² Dopo gli attacchi terroristici del 13 novembre 2015 a Parigi, la Francia ha invocato l'attivazione dell'articolo 42, paragrafo 7, del Trattato sull'Unione europea (TUE), la cosiddetta clausola di assistenza reciproca, per la prima volta dall'introduzione del Trattato di Lisbona, entrato in vigore il 2009. La Francia voleva che gli Stati membri dell'Unione Europea (UE) lo aiutassero a combattere il cosiddetto gruppo Stato Islamico di Iraq e Siria (ISIS), promotore degli attacchi. La Francia avrebbe potuto anche chiedere assistenza attraverso l'articolo 5 del Trattato Nord Atlantico (NATO) o la clausola di solidarietà dell'UE, che è specificamente progettata per rispondere agli attacchi terroristici. Tuttavia, la Francia ha scelto l'articolo 42, paragrafo 7, rispetto alle alternative, perché era più flessibile e presentava un bagaglio politico inferiore. Ha inoltre permesso alla Francia di chiedere che altri Stati membri contribuissero ulteriormente alle sue varie azioni di politica estera e di sicurezza in tutto il mondo per alleviare l'onere che le stavano imponendo. In altre parole, la clausola ha consentito alla Francia di chiedere una “solidarietà forzata”, che andava oltre ciò che avrebbe potuto chiedere ai suoi partner in circostanze meno straordinarie. Per uno approfondimento, N.I.M. NOVÁKY, *The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity*, in *European Foreign Affairs Review*, 3, 2017, p. 357 ss.

⁷³ Si veda su tutti, per un riferimento ai fatti di cronaca riportati, M. SERAFINI, *PlayStation e Isis, cosa sappiamo delle comunicazioni del Califfato*, in *Corriere della sera*, 27 novembre 2015. L'articolo è disponibile in formato digitale al link: https://www.corriere.it/tecnologia/cyber-cultura/15_novembre_27/playstation-isis-chat-comunicazioni-califfato-3ce82c5e-94f2-11e5-a313-3e29108494fd.shtml?refresh_ce-cp.

⁷⁴ Per un approfondimento, M. LAKOMY, *Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment*, in *Studies in Conflict & Terrorism*, 4, 2019, pp. 383-406; A. AL-RAWI, *Video Games, Terrorism, and ISIS's Jihad 3.0*, in *Terrorism and Political Violence*, 4, 2018, pp. 740-760.

In un simile contesto, gli Stati, l'Unione europea e gli organismi internazionali hanno reagito collocando il tema del terrorismo internazionale e delle relative strategie di contrasto⁷⁵ in cima alle proprie priorità, al fine di dare una seria risposta ad una emergenza divenuta nel tempo centrale poiché mina la sicurezza della popolazione e la tenuta dello Stato di diritto⁷⁶.

Da ciò emerge prepotentemente l'importanza di un patrimonio conoscitivo, di mezzi e di persone in grado di contrastare il fenomeno del "cyber terrorismo"⁷⁷, ma che al tempo stesso sia regolato in maniera tale da poter garantire i diritti fondamentali della persona⁷⁸.

⁷⁵ Per uno studio sulle strategie di contrasto al terrorismo internazionale, basato su recenti dati estratti dal *Global Terrorism Database*, H. FUJITA, A. GAETA, V. LOIA, F. ORCIUOLI, *Hypotheses Analysis and Assessment in Counterterrorism Activities: A Method Based on OWA and Fuzzy Probabilistic Rough Sets*, in *IEEE Transactions on Fuzzy Systems*, 28, 2020, p. 831 ss.

⁷⁶ Cfr., G. ZICCARDI CAPALDO, M. NINO, *Sistema ONU di contrasto al terrorismo e deficit delle garanzie procedurali e processuali*, in AA.VV., *Studi in onore di Modestino Acone*, vol. I, Napoli, 2010, p. 301 ss.

⁷⁷ Il termine *cyberterrorism* è stato coniato da B. COLLIN, *The Future of Cyberterrorism*, in *Crime and Justice International*, marzo 1997, p. 15-18, in cui descrive diversi ipotetici scenari ove sono rappresentati attacchi realizzabili attraverso le nuove tecnologie e la rete.

⁷⁸ Sul bilanciamento tra esigenze securitarie e diritti della persona nel contrasto al terrorismo, tra i tanti, M. DANIELE, *Le indagini informatiche contro il terrorismo. Bilanciamenti difficili e timori legislativi*, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, (a cura di R. WENIN, G. FORNASARI), Napoli, 2017, p. 265 ss.; N. GALLO, *L'attività di contrasto al terrorismo di matrice islamica. Le scelte del legislatore*, in AA.VV., *Conflittualità politico sociale intorno al Mediterraneo* (a cura di A. PANAINO), Milano, 2006, p. 33 ss.; G. DI PAOLO, «Tecnologie di controllo» e prova penale. *L'esperienza statunitense e spunti per la comparazione*, Padova, 2008, p. 67 ss.; V. FANCHIOTTI, *Il dopo 11 settembre e l'Usa patriot act: lotta al terrorismo e «effetti collaterali»*, in *Quest. Giust.*, 2004, p. 283 ss.; R.E. KOSTORIS, *Il nuovo "pacchetto" antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo* (a cura di R. KOSTORIS, F. VIGANÒ), Torino, 2015, p. XV ss.; R.E. KOSTORIS, R. ORLANDI, *Introduzione*, in AA.VV., *Contrasto al terrorismo interno e internazionale* (a cura di R.E. KOSTORIS, R. ORLANDI), Torino, 2006, p. VII ss.; C.D. LEOTTA, *La repressione penale del terrorismo a un anno dalla riforma del D.L. 18 febbraio 2015, n. 7, conv. con modif. dalla L. 17 aprile 2015, n. 43*, in *Arch. pen.*, 2016, p. 11 ss.; A. MANNA, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in *Riv. it. dir. proc. pen.*, 2004, p. 1022; D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, 2016, p. 44 ss.; I.C. PAŞCA, *The Danger of Islamic Terrorism in Romania*, in *Journal of Eastern-European Criminal Law*, 1, 2016, p. 166 ss.; V. PATANÈ, *Recent Italian Efforts to Respond to Terrorism at the Legislative Level*, in *Journal of International Criminal Justice*, 4, 2006, p. 1166 ss.; F. VANORIO, *Il contrasto al terrorismo globale tra esigenze di prevenzione e di tutela dei diritti fondamentali*, in *Questione giustizia*, 5 gennaio 2021, disponibile al link: https://www.questionegiustizia.it/articolo/il-contrasto-al-terrorismo-globale-tra-esigenze-di-prevenzione-e-di-tutela-dei-diritti-fondamentali?idn=24&idx=17718&idlink=4&utm_source=newsletter&utm_medium=email&utm_campaign=20210109; J.A.E. VERVAELE, *The anti-terrorist legislation in the US; inter arma silent leges?*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2, 2005, p. 201 ss. Per uno studio relativo alle modalità con cui il diritto penale islamico può contrastare la criminalità informatica, A. MAGHAIREH, *Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cyber crime?*, in *International Journal of Cyber Criminology*, 2, 2008, p. 337 ss.

Di recente, nella giurisprudenza nazionale Cass., Sez. V, sentenza del 23 luglio 2020, n. 22066. Nella giurisprudenza EDU, ex multis, Corte EDU, sentenza del 2 settembre 2010, *Uzun c. Germania*, n. 35623/05; Corte EDU, sentenza del 12 gennaio 2010, *Gillan e Quinton c. Regno Unito*, n. 4158/05; Corte EDU, sentenza del 27 settembre 1995, *McCann e altri c. Regno Unito*, n. 18984/91; Corte EDU, sentenza del 20 dicembre 2011, nn. 18299/03, 27311/03; Corte EDU, sentenza del 13 aprile 2017, *Tagayeva e altri c. Russia*, nn. 26562/07, 14755/08, 49339/08; Corte EDU, sentenza del 19 febbraio 2009, *A. e altri c. Regno Unito*, n. 3455/05; Corte EDU, sentenza del 26 gennaio 2012, *Berasategi c. Francia*, n. 29095/09; Corte EDU, sentenza del 27 novembre 2008, *Saldut c. Turchia*, n. 36391/02; Corte EDU, sentenza del 12 maggio

Andrebbe, quindi, individuato un corretto bilanciamento tra interessi contrapposti al fine di scongiurare fenomeni negativi come quello innescato da alcune funzioni di *dataveillance*, fondati su strumenti lesivi o limitativi del diritto alla riservatezza, come ad esempio la creazione di enormi *database* in cui confluiscono i dati delle persone utilizzati al fine di ottenere informazioni utili a contrastare il terrorismo e la criminalità organizzata, ma ottenuti ufficialmente per scopi commerciali⁷⁹.

Resta un dato indiscutibile: la diffusione di nuove forme di criminalità e di terrorismo che operano mediante l'utilizzo del cyberspazio. Per “cyber-terrorismo” si può quindi intendere l'uso di internet e dei suoi spazi virtuali per fini terroristici ovvero per diffondere la paura ed il panico nella popolazione, destabilizzando l'ordine e la sicurezza pubblica, per ragioni politiche, ideologiche o religiose.

Secondo una definizione NATO del 2008, il *cyber-terrorismo* si serve «della rete o di comunicazioni sufficienti per ingenerare la distruzione o interruzione, per creare paura o per intimidire i membri di una società in un obiettivo ideologico in ambito politico e giuridico»⁸⁰.

Il “cyber-terrorismo” è caratterizzato da alcune componenti comuni sia alla criminalità informatica sia al terrorismo di stampo tradizionale⁸¹, ma da queste se ne distacca per talune circostanze. Infatti, la dottrina americana parla di convergenza tra *cyberspace* e terrorismo, con particolare riferimento ad attacchi illeciti e minacce di attacco contro computer, reti e informazioni ivi contenute allo scopo di intimidire o costringere un governo o la sua popolazione a realizzare obiettivi politici o sociali⁸².

Dal punto di vista oggettivo, il *cyber* terrorismo si contraddistingue per: la presenza di strumenti informatici, elettronici e/o strutture internet e loro dati, utilizzati o come strumenti per concludere un attacco o come obiettivi; una motivazione di stampo

2005, *Öcalan c. Turchia*, n. 46221/099; Corte EDU, sentenza del 25 settembre 2012, *El Haski c. Belgio*, n. 649/08; Corte EDU, sentenza del 2 ottobre 2008, *Leroy c. Francia*, n. 36109/03; Corte EDU, sentenza del 27 giugno 2017, *Belkacem c. Belgio*, n. 34367/14.

⁷⁹ Più diffusamente, sul nesso tra esigenze di contrasto al terrorismo e tutela della *privacy* e dei dati personali, M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012, p. 3 ss.

⁸⁰ Cfr., G. DI DONATO, *Il cyberterrorismo di matrice religiosa*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 219.

⁸¹ In tal senso, R. FLOR, *Cyber-terrorismo e diritto penale in Italia*, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali* (a cura di R. WENIN, G. FORNASARI), Napoli, 2017, p. 335.

⁸² Così, D.E. DENNING, *Cyberterrorism: The Logic Bomb versus the Truck Bomb*, in *Global Dialogue*, 4, 2000, p. 29. Infatti, secondo l'A. «Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not». Altra parte della dottrina americana ha anche indicato ipotesi concrete che fungono da esempio per l'individuazione del cyberterrorismo. Tra di esse, si annoverano gli attacchi ai sistemi informatici di controllo del traffico aereo, del ciclo di produzione dei medicinali e del livello di pressione nelle condutture di gas naturali. Cfr., B. COLLIN, *The Future of Cyberterrorism*, cit., p. 15. Sul punto, v. anche, F. CAJANI, *Le indagini informatiche per i reati di cyberterrorismo*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1524 ss.; S. PIETROPAOLI, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Rivista di filosofia del diritto*, 2, 2019, p. 391.

terroristico-ideologico; l'esecuzione dell'azione da parte di una persona o un gruppo di persone non legate ad uno Stato né ad una agenzia governativa.

Dal punto di vista soggettivo, secondo parte della dottrina è possibile parlare di *cyber* terrorismo ogni qual volta un terrorista utilizza *internet* o nuove tecnologie digitali⁸³. Altri, invece, ritengono che sia necessario un approccio *actor-neutral*, secondo cui bisogna valutare la natura intersoggettiva e costruita della conoscenza da parte dei terroristi, ovvero le motivazioni ed esperienze personali dei terroristi, la loro mentalità e visione del mondo⁸⁴.

Altri ancora considerano *cyber* terrorismo l'utilizzo di strumenti di reti di computer per il danneggiamento o la messa fuori uso di infrastrutture critiche. Questo approccio – detto *target approach* – si concentra sull'obiettivo, evitando qualsiasi tipo di approfondimento relativo all'esecutore, all'azione o alla sua motivazione⁸⁵.

Infine, per individuare ipotesi di *cyber* terrorismo, c'è chi ritiene che sia necessario considerare alcuni elementi, senza prevedere una gerarchia. Gli elementi del *matrix approach* sono persone (o gruppi); posti (esecutori, complici e vittime); metodologie/modalità di azioni, strumenti, obiettivi, affiliazioni e motivazioni⁸⁶. Altri, pur seguendo lo stesso metodo, integrano l'elenco con l'origine dell'attacco-gravità (identità dell'attaccante), origine dell'attacco al sistema (tipo di IT e sistemi), motivazione, obiettivo-gravità (popolazione, organizzazione, identità), obiettivo-tipologia, risultato desiderato e risultati ottenuti⁸⁷.

Seguendo tali impostazioni, il *cyber* terrorismo non va confuso né con la criminalità informatica o *cybercrime*, né con la *cyber war*⁸⁸, poiché divergenti per motivazioni ed intenzioni, seppur possano verificarsi situazioni *borderline* non perfettamente inquadrabili in una delle tre categorie individuate.

Le forme con cui si manifesta possono essere due: o attraverso attività di propaganda o attraverso attività diretta.

Con l'attività di propaganda si può intendere la diffusione del pensiero o di una ideologia al fine di ottenere consenso popolare, utilizzando mezzi di comunicazione capaci di raggiungere un'ampia platea. Scopo di essa è tentare di convincere quante più persone possibili ad aderire all'organizzazione e ad apportare un proprio contributo⁸⁹. La

⁸³ K.C. DESOUZA, T. HENSGEN, *Semiotic emergent framework to address the reality of cyberterrorism*, in *Technol. Forecast. Soc. Change*, 4, 2003, p. 388.

⁸⁴ M. STOHL, *Dr. Strangeweb: Or How They Stopped Worrying and Learned to Love Cyber War*, in T.M. CHEN, L. JARVIS, S. MACDONALD (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, 2014, pp. 85-102; R. HÜLSSE, A. SPENCER, *The Metaphor of Terrorism: Terrorism Studies and the Constructivist Turn*, in *Security Dialogue*, 6, 2008, pp. 571-592.

⁸⁵ In argomento, L. AYALA, *Cybersecurity Lexicon*, New York, 2016.

⁸⁶ Così, S. GORDON, R. FORD, *Cyberterrorism? Symantec Security Response White Paper*, Cupertino, 2003.

⁸⁷ G.A. ARIELY, *Adaptive Responses to Cyberterrorism*, in T.M. CHEN, L. JARVIS, S. MACDONALD (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, 2014, pp. 175-195.

⁸⁸ Sulla *cyberwar*, G. SUFFIA, *Geografia delle cyberwars: uomini e Stati alla prova dello spazio digitale*, Milano, 2018, p. 23 ss.

⁸⁹ Un esempio di efficace campagna di reclutamento è quello del Califfato islamico in Siria ed Iraq, proclamato nel luglio 2014 da Abu Bakr Al-Baghdadi. La campagna mediatica senza precedenti che ne è susseguita, ove si mostravano i successi ottenuti sul campo dalle forze armate, unite al "sapiente" uso professionale e manipolativo dei social network, hanno aumentato l'impatto e l'effetto del Califfato su reclutamento, finanziamento, intimidazione e guerra psicologica. L'uso delle piattaforme social ha permesso al Califfato di raggiungere un vasto pubblico, sfruttando la massima libertà fornita da internet. L'eccezionale diffusività delle informazioni può essere rappresentata anche solo affermando che circa 4.000 foto e sessanta video pubblicati dallo Stato islamico sono stati trovati sul cellulare di Sayfullo

propaganda da parte delle organizzazioni criminali può essere veicolata attraverso numerosi canali. Si spazia dai semplici blog, ai social network⁹⁰ (Facebook, Instagram, Twitter, Tik Tok), passando per app di messaggistica istantanea (Whatsapp, Telegram, Messenger, Skype, Kik, Hangout, chat di incontri, ecc.) arrivando sino agli spam e a siti dedicati, anche nel *dark web*⁹¹.

L'attività diretta consente invece di utilizzare direttamente il cyberspazio per attaccare, dimostrando la propria potenza. Gli attacchi consistono in mere dimostrazioni come il *defacement*⁹² di un sito web sino a vere e proprie intrusioni in un sistema informatico⁹³. Obiettivi possono essere raramente semplici cittadini, più spesso, invece, infrastrutture critiche di un Paese, le quali subiscono malfunzionamenti che causano il panico tra la popolazione. Altre volte le intrusioni sono compiute per sottrarre informazioni segrete ad agenzie, organi o organismi nazionali ed internazionali. Questi attacchi informatici sono potenzialmente distruttivi e spesso sono effettuati a danno di infrastrutture sensibili, come accaduto nella "vicenda Centcom"⁹⁴.

Il fenomeno terroristico, forte delle nuove potenzialità assunte grazie all'impiego degli strumenti informatici, ha acquisito rilevanza su scala mondiale ed ha posto al centro del dibattito internazionale lo sviluppo di strategie comuni di sicurezza basate sulla creazione di nuovi strumenti giuridici di prevenzione e di contrasto a livello nazionale ed internazionale⁹⁵.

Infatti, la rivoluzione del *web 2.0* – caratterizzata dal crescente coinvolgimento degli utenti nella creazione e distribuzione dei contenuti in rete – ha aumentato il rischio di attacchi cyber terroristici. Il *web* è diventato un canale privilegiato per i terroristi che

Saipov, l'Uzbeko che ha sferrato l'attacco a Manhattan nel novembre 2017, in cui sono state uccise otto persone. Per un approfondimento circa tale notizia, B. MULLER, W.K. RASHBAUM, A. BAKER, A. GOLDMAN, *Prosecutors Describe Driver's Plan to Kill in Manhattan Terror Attack*, in *New York Times*, 1 novembre 2017, disponibile al link: <https://www.nytimes.com/2017/11/01/nyregion/driver-had-been-planning-attack-in-manhattan-for-weeks-police-say.html>.

⁹⁰ Sull'uso dei social network da parte del terrorismo internazionale, E. AZANI, N. LIV, *A Comprehensive Doctrine for an Evolving Threat: Countering Terrorist Use of Social Networks*, in *Studies in Conflict & Terrorism*, 8, 2020, pp. 728-752.

⁹¹ Per uno studio sui dati raccolti, si rinvia a J. KLAUSEN, *Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, in *Studies in Conflict & Terrorism*, 1, 2015, pp. 1-22.

⁹² Si tratta di un atto illecito che consiste nel modificare la home page o le pagine interne di un sito web, al fine di creare un danno o dimostrare la propria abilità o la scarsa sicurezza di un sistema.

⁹³ Oltre alla definizione contenuta nella Convenzione di Budapest (di cui si parlerà nel prosieguo), si ritiene che, in linea generale, per sistema informatico debba intendersi la complessa struttura costituita dalle componenti *hardware* e *software*, le prime rappresentate da un insieme di elementi fisici non modificabili – quali circuiti, unità di memoria, parti meccaniche, ecc. –, e da periferiche come tastiere, scanner, monitor, stampanti, ecc.; mentre le seconde costituite dall'insieme di istruzioni e procedure necessarie per il funzionamento stesso della macchina o per farle eseguire determinate attività, e costituiti da programmi o dati memorizzati su specifici supporti. Cfr., Cass., SS.UU., sentenza del 7 settembre 2017, n. 40963.

⁹⁴ Si tratta di un attacco hacker perpetrato il 12 gennaio 2015 dai militari dell'ISIS ai danni della banca dati dell'account *twitter* @Centcom, riconducibile al Comando statunitense che controlla le operazioni contro lo Stato islamico in Siria ed Iraq.

⁹⁵ Per un approfondimento, R. FLOR, *Il contrasto al terrorismo nell'era delle nuove tecnologie e i meccanismi di cooperazione fra settore pubblico e settore privato*, in AA.VV., *Scritti in onore di Luigi Stortoni* (a cura di M. MANTOVANI, F. CURI et al.), Bologna, 2016, pp. 513- 546; I. MARCHI, "Emergenza terrorismo": strategie di prevenzione e contrasto anche in prospettiva europea, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali* (a cura di R. WENIN, G. FORNASARI), Napoli, 2017, p. 69 ss.; U. SIEBER, P. BRUNST, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions*, Strasbourg, 2007.

vogliono raggiungere persone non ancora esposte alle attività di propaganda e di reclutamento al fine di coinvolgerle negli attacchi⁹⁶. Il *web*, inoltre, rappresenta un mezzo per sferrare potenti attacchi terroristici.

Di ciò è pienamente consapevole l'Unione europea, la quale con la risoluzione 2018/C 415/04 "Sull'urgenza di nuove misure per la lotta al terrorismo internazionale" ha evidenziato la pericolosità delle nuove organizzazioni terroristiche. Queste ultime, attraverso *Internet*, l'uso del *dark web*, dei social media e delle TIC, hanno trovato il modo di diffondere la loro propaganda, ottenere finanziamenti e diventare autentiche reti globali senza bisogno di una base fisica⁹⁷.

È possibile, dunque, concludere come si sia realizzata una convergenza fra cyberspazio e terrorismo⁹⁸ che sembra ricomprendere anche le c.d. *politically motivated hacking operations* realizzate per causare gravi danni alle istituzioni, all'economia, alla vita ed all'integrità fisica⁹⁹.

3. Il cyberspazio come luogo di consumazione dei reati

3.1. Da Internet...

La criminalità che opera con strumenti informatici, inclusi nel novero delle nuove tecnologie, non può che trovare un proprio terreno di elezione nel cyberspazio. È, dunque, necessario conoscere e scoprire gli ambienti, anche nascosti, ove si consumano i *cybercrime*, al fine di sviluppare strumenti di natura processuale – in particolare di tipo investigativo – utili al celere contrasto del fenomeno in funzione sia preventiva sia repressiva.

L'impiego dell'informatica e della rete si è rivelato estremamente prezioso nella lotta al crimine¹⁰⁰, nonostante il progresso tecnologico inarrestabilmente veloce tenda a rendere obsolete nel breve periodo non solo le tecnologie utilizzate ma anche la legislazione, se troppo puntuale.

La realtà sviluppatasi con internet è particolarmente complessa perché ha cambiato gli schemi sociali preesistenti. Si tratta di un progresso che ha o sostituito o modificato i tradizionali modelli socio-culturali in un'ottica spiccatamente innovativa, e con essi,

⁹⁶ Cfr. E. AZANI, N. LIV, *A Comprehensive Doctrine for an Evolving Threat: Countering Terrorist Use of Social Networks*, cit., p. 729; K.A. RUANE, *The Advocacy of Terrorism on Internet: Freedom of Speech Issues and the Material Support Status*, in *Congressional Research Service*, 8 settembre 2016, pp. 1-23; A.N. SCHUPACK, *The Arab-Israel Conflict and Civil Litigation Against Terrorism*, in *Duke Law Journal*, 1, 2010, pp. 207-247.

⁹⁷ Cfr., lett. K) del considerando, Risoluzione "Sull'urgenza di nuove misure per la lotta al terrorismo internazionale", (2018/C 415/04).

⁹⁸ Di convergenza tra cyberspazio e terrorismo si parla anche in CYBERCRIME CONVENTION COMMITTEE (T-CY), *Guidance Note #11 – Aspects of Terrorism covered by the Budapest Convention*, in www.coe.int.

⁹⁹ In tal senso, D.E. DENNING, *Activism, Hacktivism and Cyberterrorism: The Internet as Tool for Influencing Foreign Policy*, in J. ARQUILLA, D. RONFELDT (eds.), *Networks and networks. The influence of terror, crime and militancy*, Santa Monica, 2001, pp. 239-288, e specificamente p. 241.

¹⁰⁰ In tema, S. PORTESI, *Potential Applications of Advances in Technology to Prevention and Response to Cases of Terrorism and Criminality: the Role of Information and Communication Technologies*, in *Cyberspazio e diritto*, 2, 2004, p. 159 ss.

anche il mondo del diritto, sempre più coinvolto in un complicato rapporto con il progresso scientifico¹⁰¹.

Secondo la dottrina¹⁰², la nuova realtà internettiana ha agito su quattro contesti sociali: Nell'ambito del "contesto ideologico" ha espresso una libertà costituzionalmente garantita attraverso la libera circolazione nel *web* e nel *deep web*¹⁰³; nel ramo del "contesto tecnologico moderno" ha consentito il trasferimento della sfera privata personale nello "spazio pubblico", con la conseguente fluidificazione della distinzione tra pubblico e privato, dovuto all'imponente quantità di dati-informazioni espressione della personalità dell'individuo riversatasi in "spazi" quali i *social network*, *social media* e *web*; nella sfera del "contesto giuridico" ha posto il nuovo tema della "regola tecnologica" che disciplina il suo utilizzo, le sue modalità applicative o i suoi effetti nella società; nel settore del "contesto delle scelte politico-criminali" ha consentito l'emersione del dilemma relativo all'equilibrio tra la sfera dei diritti e delle libertà individuali e quella dei poteri statuali, compreso quello di punire.

In uno scenario così complesso, caratterizzato dall'innovazione scientifica e tecnologica, imparare a conoscere e riconoscere celermente gli spazi in cui si annida il crimine informatico è fondamentale al fine di contrastarne la diffusione e reprimere le condotte particolarmente lesive dei beni giuridicamente protetti.

Ciò perché la piena conoscenza delle tecnologie è il solo modo che ha il giurista per comprendere il significato delle condotte tenute «in» e «per mezzo» di esse, ed evitare di pervenire a conclusioni giuridiche incoerenti con la realtà da normare¹⁰⁴.

I luoghi ove agiscono le nuove forme di criminalità sono stati creati – e si creano – con *internet*. Dare una definizione di *internet* è attività particolarmente complessa¹⁰⁵. Non esiste una precisa definizione unanimemente accettata dalla comunità scientifica, né le fonti normative si sono spinte sino al punto da riempire di contenuto un concetto che si presta ad una visione prismatica.

Internet è una rete di comunicazione globale e, al pari di una rete telefonica, rappresenta, in quanto tale, un sistema che consente di collegare contemporaneamente due o più dispositivi che impiegano un linguaggio comune definito "protocollo di comunicazione". Si tratta di una "rete di reti" che adopera protocolli di comunicazione comuni, oppure come una comunità di persone che utilizzano e sviluppano tali *network*, o ancora come un insieme di risorse che possono essere raggiunte via rete¹⁰⁶. Quale "regina delle reti", sarebbe una inter-rete in grado di collegare tutte le reti e di far

¹⁰¹ Parte della dottrina ritiene un paradosso da saper governare i rapporti tra scienza e diritto e delle controversie tecnico-scientifiche nel diritto e nel processo penale. Tale condizione va gestita «guardandosi dal duplice pericolo che la scienza espropri il diritto, e che il diritto ignori o rinneghi la scienza. Impresa irrealizzabile in linea di astratto principio, ma difficile nei fatti». Così, G. FIANDACA, *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale*, in *D.&Q. pubbl.*, 2005, p. 22-23. V., inoltre, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 143.

¹⁰² Cfr., R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 142.

¹⁰³ Tale libertà si manifesta mediante strumenti che aumentano esponenzialmente la potenzialità comunicativa e diffusiva.

¹⁰⁴ In tal senso, G. PICA, voce *Internet (dir. pen.)*, in *Dig. disc. pen.*, Agg. II, Torino, 2004, p. 425 ss.

¹⁰⁵ In argomento, S. MONTALDO, *Internet e commons: le risorse della rete nella prospettiva dei beni comuni*, in *Diritto dell'informazione e dell'informatica*, 2, 2013, p. 287 ss.

¹⁰⁶ In tal senso, G. PASCUZZI, voce *Internet (dir. civ.)*, in *Dig. disc. civ.*, Agg., Torino, 2000, p. 225 ss.

comunicare tra loro dispositivi diversi attraverso l'impiego di una lingua tecnica comune¹⁰⁷.

Inteso così, *internet* sarebbe una metodologia di comunicazione ipertestuale che consente l'accesso e lo scambio di qualsiasi contenuto digitale che transita su sistemi informatici connessi alla Rete composta non solo da una parte *software* ma anche da *hardware*, cioè da tutta una componentistica che funge da "sistema viario e di trasporto" su cui circolano i dati-informazioni¹⁰⁸.

A questa impostazione – che perviene alla conclusione secondo cui *internet* sia un conglomerato di *software* ed *hardware* e non un vero luogo o uno spazio – si affianca il pensiero di rilevante dottrina che ravvisa in *internet* non solo «il più grande spazio pubblico che l'umanità abbia conosciuto», ma anche «un luogo dove la vita cambia qualità e colore, dove sono possibili l'anonimato e la moltiplicazione delle identità, la conoscenza e l'ubiquità, la libertà piena e il controllo totale»¹⁰⁹. *Internet* sarebbe diventato, col tempo¹¹⁰, una realtà peculiare di un più ampio universo comunicativo¹¹¹.

Come accennato, per garantire un corretto dialogo in questo insieme di reti sono necessari protocolli tecnici comuni che consentano agli utenti di una rete di comunicare con gli utenti di altre reti ovvero di utilizzare i servizi concessi. Questo *standard* comune – una sorta di *koiné* – è il c.d. protocollo TCP/IP, acronimo di *Transmission Control Protocol/Internet Protocol*¹¹², ossia un insieme di regole pubbliche accessibili a tutti. Per

¹⁰⁷ Così, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 22.

¹⁰⁸ L'*hardware*, composto da cavi, router, server, fibra ottica, ecc., non rappresenta l'essenza di *internet* perché l'*hardware* esiste anche senza *Internet* e supporta qualunque altra forma di comunicazione telematica, in Rete o meno. Se può affermarsi che l'*hardware* e la telematica esistono anche senza *internet*, non può ritenersi vero il contrario: *internet* non esisterebbe se non fossero stati creati gli *hardware* e non fossero stati inventati i protocolli di inter-comunicazione universale fra sistemi diversi ed il *software* di comunicazione ipertestuale. Sul punto, G. PICA, voce *Internet* (dir. pen.), in *Dig. disc. pen.*, cit., p. 425 ss.

¹⁰⁹ Così, S. RODOTÀ, *Persona, libertà, tecnologia. Note per una discussione*, in *D.&Q. pubbl.*, 2005, p. 25. Vi è chi ha paragonato *internet* ad una chiesa dove chiunque può entrare qualora ne accetti i principi e la filosofia si da dividerne i benefici. Per questo paragone, E. KROL, *The Whole Internet: User's Guide & Catalog*, Sebastopol, 1992.

¹¹⁰ I padri di *internet* sono Robert Kahn e Vinton G. Cerf. La genesi di *Internet* viene fatta risalire ad un esperimento intrapreso ai tempi della "guerra fredda" nel 1969 dal Dipartimento della Difesa statunitense, il quale commissionò la creazione di ARPANET - una rete di computer militare – all'agenzia di Progetti e ricerca Avanzati (Advanced Research Project Agency- ARPA) – successivamente ribattezzata Defense Advanced Research Projects Agency (DARPA) – per tentare di interconnettere la propria rete, denominata ARPANET, con alcune reti radio e satellitari. Il progetto aveva scopi militari: l'obiettivo era quello di riuscire a comunicare in caso di malfunzionamento o di attacco nemico senza che vi fosse un unico centro che potesse essere oggetto di aggressione termonucleare e senza che i messaggi potessero essere intercettati e bloccati. Sorse così un sistema che inviava informazioni divise in «pacchetti» di dati che potevano viaggiare lungo rotte differenti per poi essere ricongiunti alla destinazione finale. Tale sistema (Transmission Control Protocol/Internet Protocol o TCP/IP) consentiva ai dati, in caso di problemi o danneggiamenti ad un computer, di pervenire comunque al destinatario sfruttando linee alternative. Agli inizi degli anni Ottanta l'esercito americano lasciò ARPANET, che in seguito diventò *Internet*. Istituzioni accademiche e altre agenzie governative si unirono subito a *Internet* collegando le reti dei loro computer al sistema, sino alla totale e libera apertura alla collettività. Cfr., sull'argomento, K. HAFNER, M. LYON, *Where Wizards Stay up Late: The Origins of the Internet*, New York, Touchstone, 1998; G. PASCUZZI, voce *Internet* (dir. civ.), in *Dig. disc. civ.*, cit., p. 225 ss.; G. PICA, voce *Internet* (dir. pen.), in *Dig. disc. pen.*, cit., p. 425 ss.

¹¹¹ Cfr., P. COSTANZO, voce *Internet* (dir. pubbl.), in *Dig. disc. pubbl.*, Agg., Torino, 2000, p. 347 ss.

¹¹² Sul tema, D. DE JUDICIBUS, *TCP/IP*, in *Internet news*, 2, 1996, p. 74 ss.; V. FROSINI, *Telematica ed informatica giuridica*, in *Enc. dir.*, XLIV, Milano, 1992, p. 60 ss.; S. GOSWAMI, *Internet protocols. Advances, Technologies and Applications*, Berlino, 2003; G. PASCUZZI, *Il diritto nell'era digitale*, III ed.,

poter comunicare mediante protocollo è necessario che ciascun dispositivo sia dotato di un numero identificativo, denominato IP, una sorta di “denominazione alfanumerica” del dispositivo, dato che non possono esistere due IP identici collegati ad *internet* nello stesso momento.

Se si considera la peculiarità dell’indirizzo IP si può concludere che quest’ultimo assume un ruolo centrale in sede di indagini penali, poiché potrebbe rappresentare il punto di partenza per queste, consentendo di individuare il dispositivo collegatosi ad *internet*¹¹³ ed il soggetto agente.

Peculiarità di *internet* sono l’ontologica sovranazionalità¹¹⁴, la struttura acentrica ed acefala¹¹⁵, nonché la presenza di caratteristiche come l’ipertestualità, l’ipermedialità e l’interattività¹¹⁶.

Proprio tali caratteristiche hanno fatto emergere consapevolmente dubbi circa l’efficacia e l’effettività di norme cristallizzate da applicare a fenomeni tecnologici che mutano con incredibile velocità. Infatti, in passato, secondo alcuni sarebbe stato preferibile lasciare che internet si autoregolamentasse attraverso codici di autodisciplina di generale applicazione (la c.d. netiquette)¹¹⁷, senza agire con una normativa inattuabile, in ragione della internazionalità di cui si connota il sistema.

In realtà, a chi scrive sembra alquanto complicato che la rete possa autoregolarsi, soprattutto in aree come quella penale, alla cui base si colloca l’interesse alla tutela di beni giuridicamente e costituzionalmente protetti. Ciò non è frutto di astrattismo, ma risultato di una empirica osservazione della realtà fenomenica.

È evidente però che, innanzi ad un sistema caratterizzato dalla sovranazionalità, l’azione dei singoli ordinamenti statuali rischia di essere priva di effetti. Invero, una prima e forte risposta non può che aversi da parte delle istituzioni sovranazionali, così come di

Bologna, 2016, p. 23 ss.; ID., *Scoperte scientifiche, invenzioni e protocolli relativi a Internet*, in *AIDA*, 5, 1996, p. 161 ss.; ID., *Cyberdiritto. Guida alle banche dati italiane e straniere, alla rete Internet e all’apprendimento assistito da calcolatore*, Bologna, 1995; G. PICA, voce *Internet (dir. pen.)*, in *Dig. disc. pen.*, cit., p. 425 ss.; G. RICHERI, *Autostrade dell’informazione*, in *Economia della cultura*, 2, 1994, p. 116 ss.

¹¹³ Per un approfondimento, anche relativo al tema dell’indirizzo IP, *ex multis*, G. FORTINO, P. TRUNFIO, *Internet of Things Based on Smart Objects*, Berlino, 2004; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 22 ss.

¹¹⁴ Così, G. PICA, voce *Internet (dir. pen.)*, in *Dig. disc. pen.*, cit., p. 425 ss.

¹¹⁵ In questi termini, P. COSTANZO, *Le nuove forme di comunicazione in rete: Internet*, in *Informatica e Diritto*, 1997, p. 25.

¹¹⁶ Per ipertestualità si intende la condizione di un documento contenente almeno un riferimento visibile ad un altro dell’insieme dei documenti al quale il primo appartiene o a qualsiasi altro documento tra quelli pubblicati in Internet. Questo riferimento o rinvio si chiama *hyperlink* (collegamento ipertestuale) e di solito viene rappresentato sotto forma di un brano di testo sottolineato ed evidenziato con colore diverso. Cliccando sul collegamento ipertestuale, il programma di navigazione «salta» direttamente sul documento rinvio. L’ipertesto costituisce la tecnica su cui si basa il World Wide Web, uno degli «spazi» in cui è suddivisa Internet; con il termine ipermedialità si fa riferimento alla situazione in cui, attraverso gli *hyperlinks*, si realizza non solo un collegamento diretto tra testi scritti, ma anche con qualsiasi altro genere di forma comunicativa o «mediale», come suoni, immagini statiche o in movimento, riprese in tempo reale, ecc.; infine, l’interattività è la capacità del medium considerato di consentire un dialogo bidirezionale tra fonte dell’informazione ed utente oppure tra utenti, com’è, del resto, il caso più noto del telefono. Cfr., P. COSTANZO, voce *Internet (dir. pubbl.)*, in *Dig. disc. pubbl.*, cit., p. 347 ss.

¹¹⁷ Cfr. la guida alla *netiquette* di A. Rinaldi, richiamata da molte pagine Web: ad esempio, <http://www.efluxa.it/netiquette/>; <http://www.inferentia.it/netiquette/>; <http://www.fau.edu/netiquette/> net/. V. anche: <http://www.onlinenetiquette.com/>; <http://www.nic.it/NA/netiquette.txt>; <http://www.kaqs.org/rfcs/rfc1855.html>.

fatto sta avvenendo sia nell'area del diritto penale sostanziale, sia nell'area del diritto processuale penale.

3.2. ... *al cyberspace*

Internet è composto anche da uno spazio detto *cyberspace*. Il cyberspazio è uno spazio a-temporale ed a-territoriale che consente la delocalizzazione delle risorse e la pianificazione, nonché lo svolgimento di operazioni programmate dall'utente.

L'utente che opera all'interno del *cyberspace* non ha esigenza di un collegamento o un contatto fisico con un'altra persona o con un altro sistema informatico e può svolgere un'operazione complessa, pur essendo presente contemporaneamente in più spazi informatici. Questo spazio ha una natura ibrida perché è al tempo stesso sia "virtuale" sia "reale" e rappresenta un luogo non solo ove l'individuo può esprimere le proprie libertà, ma anche un posto ove persone reali possono commettere reati «rispetto al quale Internet [...] costituisce lo "strumento di accesso o di utilizzo"»¹¹⁸.

Dare una definizione precisa e comunemente accettata di *cyberspace* è particolarmente complesso: uno studio ha infatti rivelato che esistono ben 28 definizioni diverse¹¹⁹.

Una prima definizione venne fornita nel 1984 da William Gibson, il quale definì lo spazio cibernetico – ambiente artificiale, unico ad essere stato creato dall'uomo – come «un'allucinazione vissuta consensualmente ogni giorno da miliardi di operatori legali, in ogni nazione, da bambini a cui vengono insegnati i concetti matematici. Una rappresentazione grafica di dati ricavati dai banchi di ogni computer del sistema umano. Impensabile complessità. Linee di luce allineate nel non-spazio della mente, ammassi e costellazioni di dati. Come le luci di una città, che si allontanano»¹²⁰.

Altri lo definiscono come «un dominio globale all'interno dell'ambiente informatico il cui carattere distintivo e unico è caratterizzato da un uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare, e sfruttare le informazioni attraverso sistemi interdipendenti e interconnessi che utilizzano le tecnologie delle informazioni e delle comunicazioni»¹²¹.

Altri ancora ritengono che il *cyberspace* sia un *medium* virtuale e intangibile, la cui natura eterogenea è rappresentare questa realtà su tre livelli: fisico, sintattico e semantico¹²². C'è poi chi, pur conservando la struttura a triplice stratificazione, parla di livello fisico, logico e sociale¹²³.

¹¹⁸ Sul punto, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 143.

¹¹⁹ Cfr., F. KRAMER, S. STARR, L. WENTZ (eds), *Cyberpower and National Security*, Washington (D.C.), 2009.

¹²⁰ «A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concept. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding». Cfr. W. GIBSON, *Neuromancer*, New York, 1984.

¹²¹ D.T. KUEHL, *From Cyberspace to Cyber-power: Defining the Problem*, in F. KRAMER, S. STARR, L. WENTZ (eds.), *Cyberpower and National Security*, Washington (D.C.), 2009.

¹²² Così, M.C. LIBICKI, *Cyberdeterrence and Cyberwarfare*, Santa Monica (CA), 2009, p. 11 ss.

¹²³ Secondo tale rappresentazione fornita dal Department of the Army Headquarters, United States Army Training and Doctrine Command 2010, il primo strato (quello fisico) è composto dai cavi sottomarini o della rete ethernet, dai router e dispositivi di scambio dati e comunicazione. Sopra di questo vi è lo strato logico realizzato dai codici che permettono all'*hardware* di funzionare e comunicare. Il terzo strato è

In assenza di una definizione legale universalmente riconosciuta, per una nozione si può far riferimento al dominio tecnico, rappresentato dalla ISO 27032:2012¹²⁴, secondo la quale viene definito come *cyberspace* (o cyberspazio): «*the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*», ossia un ambiente virtuale (o totalmente dematerializzato) definito dal «complesso delle attività realizzate dai soggetti che usufruiscono dei servizi offerti dalla rete Internet attraverso l'impiego di sistemi informatici e telematici ad essa collegati».

Il Vice Segretario della Difesa americano, William J. Lynn III, nel 2010 ha affermato che il *cyberspace* rappresenta il «quinto dominio della conflittualità», insieme con terra, mare, aria e spazio¹²⁵. Rispetto, però, ai tradizionali domini, esso è stato costruito dall'uomo ed è dotato di peculiari caratteristiche che lo differenziano di gran lunga dagli altri. Quello cibernetico si presenta come uno spazio in continua evoluzione, strutturale e funzionale, e perciò potenzialmente pericoloso, perché luogo fertile per la proliferazione di reati, un nuovo “terreno di guerra”, in cui non si combatte con le tradizionali armi, ma i mezzi militari diventano le operazioni cibernetiche, ritenute spesso violazioni del diritto internazionale¹²⁶.

Le peculiarità dello spazio cibernetico consentono la “smaterializzazione”, la “velocizzazione”, la “deteritorializzazione”, l’“ubiquità” e la “detemporalizzazione” delle condotte concrete, che prescindono o si distanziano dalle caratteristiche fisiche dei comportamenti o dai fattori esterni¹²⁷. Questo comporta una recrudescenza ed una maggior invasività di tali reati nella sfera personale delle persone offese, o comunque una spiccata pervasività alla lesione dei beni giuridici costituzionalmente protetti¹²⁸.

Si aggiunga, sul versante strettamente processuale, la maggior difficoltà nella formazione della prova – sia essa rappresentativa, sia essa indiziaria – che riesca pienamente a dimostrare non solo l'avvenuta consumazione del reato, ma soprattutto l'autore di esso.

Ed invero, tenuto conto dell'estrema difficoltà sovente manifestatasi nell'individuazione dell'autore del reato, dovuto spesso alla carenza di strumentazione

composto dal livello sociale che consiste nell'interazione tra gli utenti online (persone fisiche) e, sempre più spesso, tra apparecchi. Questi “tre livelli” vanno a costituire la prima cornice della mappatura dello spazio cibernetico. Tuttavia, l'elemento essenziale che distingue la geografia del dominio cibernetico dalle altre realtà è rappresentato dal suo carattere artificiale ed ibrido, ritenuto «molto più mutevole rispetto ad altri ambienti; a differenza delle montagne e degli oceani statici, le parti del cyberspace possono essere attivate e disattivate con un semplice click». In tal senso, G.J. RATTRAY, *An Environmental Approach to Understanding Cyberpower*, in F. KRAMER, S. STARR, L. WENTZ (eds), *Cyberpower and National Security*, Washington (D.C.), 2009.

¹²⁴ <http://www.iso27001security.com/html/27032.html>. Cfr., G. SPECCHIO, *Analisi di contesto del cyberspace (I parte)*, in *Sicurezza & Giust.*, 3, 2019, p. 11.

¹²⁵ Sul punto, L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, 1, 2018, p. 61 ss.; M. MIRTÌ, *La disciplina giuridica del cyberspace*, in *Opinio Juris*, 23 novembre 2016;

¹²⁶ In questa direzione, F. SPIEZIA, *Attacco all'Europa*, cit., p. 183.

¹²⁷ In tal senso, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 143; ID., *I limiti del principio di territorialità nel cyberspace. Rilevi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. e proc.*, 10, 2015, p. 1291 ss.; L. PICOTTI, *Sicurezza, informatica e diritto penale*, in AA.VV., *Sicurezza e diritto penale* (a cura di M. DONINI, M. PAVARINI), Bologna, 2011, p. 217 ss., p. 223-224.

¹²⁸ Invero, data la sua atterritorialità, il *cyberspace* si presenta come uno spazio unitario, che sfugge al dominio dei singoli Stati e in cui risultano inutilizzabili le norme sulla ripartizione della giurisdizione e della competenza comunemente applicate. Su questo aspetto, F. SPIEZIA, *Attacco all'Europa*, cit., 185.

tecnologicamente avanzata in possesso degli operatori di polizia giudiziaria, ad una scarsa formazione di questi ultimi, o più semplicemente ad una maggiore preparazione dei criminali nell'area dell'informatica, la Corte di cassazione, in tema di procedimento cautelare avviato per un reato informatico o cibernetico in senso ampio – come nel caso dell'estorsione online¹²⁹ – ha più volte ribadito il principio secondo cui «la gravità degli indizi¹³⁰ di colpevolezza postula una considerazione non frazionata ma coordinata degli stessi, che consenta di verificare se la valutazione sinottica di essi sia o meno idonea a sciogliere le eventuali incertezze o ambiguità discendenti dall'esame parcellizzato dei singoli elementi di prova, e ad apprezzare quindi la loro effettiva portata dimostrativa e la loro congruenza rispetto al tema di indagine prospettato nel capo di imputazione provvisoria»¹³¹.

3.3. Deep web e dark web

Il *cyberspace* è diventato un ambiente ideale e privilegiato per realizzare molteplici, diverse e nuove forme di *cybercrime* da parte di criminali che acquisiscono competenze sempre maggiori in tali ambiti¹³².

¹²⁹ Sul reato di estorsione commesso con mezzi informatici o telematici (estorsione online o informatica o digitale oppure *cyber-estorsione*) v., M. LUBERTO, "Sex-torsion" via web e minaccia a mezzo ransomware: la nuova frontiera del delitto di estorsione, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 723 ss.

¹³⁰ Sul concetto di indizio, *ex multis*, A. BARGI, *Le prove e le decisioni*, in AA.VV., *Procedura penale* (a cura di A. GAITO), Milano, 2018, p. 352; A. BERNASCONI, *Sistema probatorio e disposizioni generali*, in AA.VV., *Manuale di diritto processuale penale*, Torino, 2015, p. 251; F. CARNELUTTI, *Lezioni sul processo penale*, Roma, 1947, p. 210; ID., *Diritto e processo*, Napoli, 1958, p. 129; F. CORDERO, *Procedura penale*, Milano, 2012, p. 585 ss.; A.A. DALIA, M. FERRAIOLI, *Manuale di diritto processuale penale*, Padova, 2018, p. 307 ss.; F.R. DINACCI, *Le regole generali delle prove*, in AA.VV., *Procedura penale. Teoria e pratica del processo*, (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), II, 2015, p. 811; O. DOMINIONI, *Il corpo del diritto delle prove*, in AA.VV., *Procedura penale*, Torino, 2017, p. 264 ss.; P. FERRUA, *Studi sul processo penale*, Torino, 1992, p. 53; V. GREVI, G. ILLUMINATI, *Prove*, in AA.VV., *Compendio di procedura penale* (a cura di G. CONSO, V. GREVI e M. BARGIS), Padova, 2018, p. 310; G. LOZZI, *Lezioni di procedura penale*, Torino, 2018, 208 s.; G. POI, *Indizi cautelari – la valutazione degli indizi nella fase cautelare: una questione da risolvere alla luce della teoria generale della prova*, in *Giur. it.*, 1, 2017, p. 213; D. SIRACUSANO, F. SIRACUSANO, *Le prove, il procedimento probatorio e il processo*, in AA.VV., *Diritto processuale penale* (a cura di G. DI CHIARA, V. PATANÈ, F. SIRACUSANO), Milano, 2018, p. 280 s.; C. TAORMINA, *Procedura penale*, Torino, 2015, p. 315 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, Milano, 2021, p. 230 ss.; G. UBERTIS, "Prova indiziaria". Ossimoro o ridondanza da evitare, in *Argomenti di procedura penale*, Milano, 2016, p. 275 ss.; ID., *Sistema di procedura penale. Principi generali*, Torino, 2013, p. 70 ss.; ID., *La prova penale. Profili giuridici ed epistemologici*, Torino, 1995, p. 44 ss.

¹³¹ Pertanto, è necessario procedere ad una valutazione coordinata e non parcellizzata dei singoli elementi indiziari, così da verificare la valenza dimostrativa e, successivamente, procedere ad un esame globale degli stessi per valutarne la congruenza rispetto al tema di indagine prospettato. Cfr., Cass., Sez. II, sentenza del 28 febbraio 2019, n. 8794, in *Diritto di internet*, 2, 2019, p. 137, con nota di A. GAUDIERI, *Estorsione via chat e gravi indizi di colpevolezza nel procedimento cautelare*. In conformità a tale sentenza, Cass., Sez. I, sentenza del 12 aprile 2016, n. 20461, in *CED Cass.*, rv. 266941 – 01; Cass., Sez. I, sentenza del 22 settembre 2015, n. 39125, in *CED Cass.*, 264780 - 01; Cass., Sez. I, sentenza del 18 aprile 2013, n. 44324, in *CED Cass.*, rv. 258321 – 01; Cass., Sez. I, sentenza del 14 marzo 2010, n. 16548, in *CED Cass.*, rv. 246935 – 01. In dottrina, G. SPANGHER, *Le misure cautelari*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), III, 2015, p. 13.

¹³² Così, R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2/3, 2007, p. 899; L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., p. 21 ss.

Da tempo il crimine sfrutta le ampie possibilità offerte dagli strumenti tecnologici, facendo un uso sistematico e capillare del *deep web* e del *dark web*, reti telematiche nascoste rispetto al *surface web*. Caratteristica principale è quella di rendere anonima l'identità degli utenti, attraverso l'occultamento degli indirizzi IP dei dispositivi connessi alla rete, e consentire la consumazione di reati, eludendo i sistemi di sicurezza¹³³.

Il *deep web* ed il *dark web* rappresentano una parte nascosta del *web* che garantisce la navigazione anonima, privata e/o clandestina all'interno della rete. Si tratta di una parte del *web* celata e quindi difficilmente sorvegliabile. *Deep web* e *dark web* non sono però la stessa cosa. Pertanto, è necessario delineare diverse definizioni e diverse caratteristiche.

È possibile suddividere il vasto oceano senza confini del *web* in tre grandi zone: il *surface web*, il *deep web* ed il *dark web*¹³⁴.

Il *surface web*¹³⁵ è solo la punta di un enorme iceberg. Si tratta della parte superficiale della rete, conosciuta dalla quasi totalità degli utenti, e rappresenta solo una piccolissima percentuale del *web*¹³⁶. Essa raggruppa tutte quelle pagine web e quei documenti che vengono indicizzati dai motori di ricerca e, pertanto, a questa parte della rete può accedere chiunque dispone di una connessione ad *internet*.

Il *deep web* è la frazione sommersa dell'iceberg. Si tratta di quella parte del *web* che i motori di ricerca tradizionali non indicizzano, per cui non è direttamente raggiungibile da tutti gli utenti. Il contenuto è accessibile anche senza particolari *software*¹³⁷ e rappresenta la parte più consistente. Si tratta di reti geografiche di telecomunicazioni private, utilizzate anche da enti pubblici¹³⁸ e aziende private per scopi legittimi. Elemento caratteristico di questo spazio è l'inaccessibilità ai contenuti mediante una semplice ricerca su un motore, poiché sono previsti codici di decriptazione di grado superiore rispetto a quelli usati nel *surface web*.

¹³³ In tal senso, F. GRAZIANI, *La ricerca della prova digitale mediante captatore informatico nella prassi degli Stati e nell'ordinamento italiano: il difficile equilibrio tra prevenzione dei reati e tutela della riservatezza informatica*, in *La Com. int.*, 3, 2019, p. 391.

¹³⁴ Sul tema, G. DI IEVA, G. ZAMBONINI, *Dal Surface al Dark Web, passando per il Deep Web (I parte)*, in *Sicurezza & Giust.*, 4, 2017, p. 49; A.D. ROMEO, *Hidden Threat: The Dark Web Surrounding Cyber Security*, in *Northern Kentucky Law Review*, 1, 2016, p. 74 ss.

¹³⁵ Cfr., G. DI IEVA, G. ZAMBONINI, *Dal Surface al Dark Web, passando per il Deep Web (I parte)*, cit., p. 49; R. FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., p. 1291 ss.; S. PIETROPAOLI, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, cit., p. 394; V. SACHETTI, *Il contrasto alla propaganda terroristica online nell'ambito dell'Unione europea: tutela attuale e prospettive future*, in *Eurojus*, 4, 2019, p. 16.

¹³⁶ Nel 2000 mentre *Bright Planet* stimava che il *web* fosse costituito da oltre 550 miliardi di risorse disponibili online, *Google* riusciva ad indicizzarne solo 2 miliardi, costituenti circa l'1% del totale. Per un riscontro, R. FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., p. 1291 ss., in particolare nota 6. V. LAGI, *Deep web, dark web e indagini informatiche*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1708.

¹³⁷ Cfr., G. DI IEVA, G. ZAMBONINI, *Dal Surface al Dark Web, passando per il Deep Web (I parte)*, cit., p. 51. Si ritiene che oggi il *deep web* costituisca il 96% del *web*. Sul tema, anche, R. FLOR, *I limiti del principio di territorialità nel cyberspace*, cit., p. 1291 ss.; B. HE, M. PATEL, Z. ZHANG, K. CHEN-CHUAN CHANG, *Accessing the Deep Web: A Survey*, Comm. ACM, 2007; R. MEGGIATO, *Il lato oscuro della rete. Alla scoperta del Deep Web e del Bitcoin*, Milano, 2014; UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI), *La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*, Torino, 2014.

¹³⁸ Comprende anche grandi reti governative e militari come SIPRNet (Secure Internet Protocol Router Network); NIPRNet (Nonclassified Sensitive Internet Protocol Router Network); CRONOS (Crisis Response Operations In NATO Operating Systems); RIPRNet (Releasable Internet Protocol Router Network); JWICS (Joint Worldwide Intelligence Communications System).

Fanno parte del *deep web* il sistema di *webmail*; le reti *intranet* aziendali, i giochi online e tutte le risorse accessibili mediante vie alternative, che utilizzano *internet* come mezzo per lo spostamento di dati dapprima frammentati e poi offuscati al fine di garantire l'anonimato in rete¹³⁹.

Al terzo livello del *web*, nella parte estrema e più nascosta di questo iceberg immaginario, si colloca il *dark web*. Il *dark web* è quella porzione del *deep web* non accessibile attraverso i normali *software*, ma il cui accesso è subordinato all'impiego di particolari programmi¹⁴⁰. È possibile definirlo come una fetta di *internet* intenzionalmente nascosta ai motori di ricerca, mediante l'impiego di indirizzi IP nascosti¹⁴¹. Oltre all'inaccessibilità ai contenuti attraverso un motore di ricerca, ulteriore caratteristica è l'anonimato¹⁴², poiché si garantisce la *privacy* verso i visitatori esterni, ed

¹³⁹ Il riferimento è al TOR network, Freenet, P2P, Osiris, Usenet ecc. Per fare un esempio, fa parte del *deep web* l'albo pretorio online, istituito con legge del 18 giugno 2009, n.69, il quale ha previsto che «gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione nei propri siti». L'albo pretorio on-line rappresenta uno spazio informatico accessibile da chiunque, ma il Garante per la protezione dei dati personali ha stabilito mediante linee guida la necessità di evitare l'indicizzazione dei documenti non pubblicati per finalità di trasparenza tramite motori di ricerca generalisti, privilegiando funzionalità di ricerca interne ai siti web delle amministrazioni. Dunque, tali documenti sono raggiungibili solo tramite un motore di ricerca interno al sito stesso, pur essendo esposti su siti pubblici, accessibili a tutti gli utenti.

Con riferimento all'uso del *deep web* e, in particolare di Tor, nelle investigazioni informatiche cfr. T. G. SHIPLEY, A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, 2014, p. 219 ss.

¹⁴⁰ La dottrina ha evidenziato che «*The darknet is not a separate physical network but an application and protocol layer riding on existing networks*». In questi termini, P. BIDDLE, P. ENGLAND, M. PEINADO, B. WILLMAN, *The Darknet and the Future of Content Protection*, in AA.VV., *Digital Rights Management* (a cura di J. FEIGENBAUM), Berlino, 2003, p. 155. V., anche, M. EGAN, *What is the Dark Web? How to Access the Dark Web. What's the Difference Between the Dark Web and the Deep Web*, in P.C. Advisor, 23 novembre 2015, <http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc3593569/>; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 30. Sulle attività del *dark web*, v. anche C.M.S. STEEL, *Stolen Identity Valuation and Market Evolution on the Dark Web*, in *International Journal of Cyber Criminology*, 1, 2019, p. 70 ss.

¹⁴¹ Cfr., G. DI IEVA, G. ZAMBONINI, *Dal Surface al Dark Web, passando per il Deep Web (I parte)*, cit., p. 49.

¹⁴² Dalla garanzia dell'anonimato derivano conseguenze positive e negative. Quanto alle prime, va osservato che l'anonimato in rete è stato riconosciuto come un diritto meritevole di protezione giuridica, così come stabilito dall'art. 10, comma 1 della Dichiarazione dei diritti in *Internet*, secondo il quale ogni «persona può accedere alla rete e comunicare elettronicamente usando strumenti anche di natura tecnica che proteggano l'anonimato ed evitino la raccolta di dati personali, in particolare per esercitare le libertà civili e politiche senza subire discriminazioni o censure». Ed inverso, nell'ambito di ordinamenti di stampo totalitario, l'uso del *dark web* – garanzia di anonimato – ha tutelato il diritto al rispetto della vita privata e familiare, la libertà di pensiero, di coscienza e di religione, nonché la libertà di riunione, di espressione e di associazione.

Dall'altro canto, però, non va taciuto l'uso distorto a cui si presta il *dark web*. Proprio la garanzia dell'anonimato consente ai criminali di nascondere la propria identità. La criminalità ha infatti individuato nel *dark web* un posto privilegiato dove concludere i propri loschi affari e commettere reati in rete o a mezzo della rete, tanto da essere diventato un luogo dove svolgere ogni tipo di attività criminosa. Per la Dichiarazione, PARLAMENTO ITALIANO, COMMISSIONE PER I DIRITTI E I DOVERI RELATIVI AD INTERNET, *Dichiarazione dei diritti in internet*, 28 luglio 2015. Per un'analisi sul tema, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 30 ss.; S. RODOTÀ, *Prefazione*, in AA.VV., *Internet, i nostri diritti* (a cura di A. MASERA, G. SCORZA), cit., p. VII; ID., *Una Costituzione per Internet?*, cit., p. 337 ss. In riferimento alle conseguenze negative, S. ATERNO, *Profili penali dell'anonimato in rete*, in AA.VV., *Sicurezza e anonimato in rete* (a cura di A. MAGGIPINTI, M. IASELLI), Milano, 2005, p. 110 ss.; A. MISSIROLI, *The Dark Side of the Web: Cyber as a Threat*, in *European Foreign Affairs Review*, 2, 2019, p. 142; A.D. ROMEO, *Hidden Threat: The Dark Web Surrounding Cyber Security*, cit., p. 73 ss.;

è celata anche l'identità di coloro che utilizzano tale spazio¹⁴³. Infine, sono possibili anche tecniche di dissimulazione dell'*ip address*, che possono far apparire provenienze "territoriali" false o errate.

Volendo fare un paragone con uno spazio reale, si potrebbe assimilare ad un "mercato nero" dove il crimine agisce indisturbato e riesce a riciclare denaro, trafficare organi e sostanze stupefacenti, vendere illecitamente armi o *malware* e *botnet*, utili per attacchi informatici, consumare reati riconducibili alla pedofilia e pedopornografia, nonché compiere attività legate alla tratta di esseri umani. Addirittura, in tale spazio, sarebbe possibile assoldare sicari che, dietro corrispettivo, consumino omicidi.

Il primo grande mercato nero che ha subito un duro colpo dalla giustizia è stato *Silk Road*¹⁴⁴, definito l'"Amazon delle droghe"¹⁴⁵. Venne chiuso definitivamente nel 2014 a seguito di una indagine internazionale, che ha stimato un volume di affari pari a circa 22 milioni di euro, e conclusasi con un processo al fondatore, Ross Ulbricht, il quale è stato condannato all'ergastolo. Per la chiusura di questo mercato nero furono necessari sei mesi di intensa attività investigativa da parte degli uomini più preparati afferenti alle agenzie statunitensi ed europee. Nella sentenza, il giudice ha affermato che «l'obiettivo principale di *Silk Road* era di essere al di sopra della legge. Nel mondo creato la democrazia non esisteva... [il fondatore era] il capitano della nave, il *Dread Pirate Roberts*»¹⁴⁶.

Di recente, le indagini nel *dark web* si sono intensificate tanto da aver portato alla chiusura del mercato nero virtuale più affidabile del web, noto come Berlusconi Market¹⁴⁷

V. SACHETTI, *Il contrasto alla propaganda terroristica online nell'ambito dell'Unione europea: tutela attuale e prospettive future*, cit., p. 16; S. SIGNORATO, *Le misure di contrasto in rete al terrorismo: black list, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo* (a cura di R. KOSTORIS, F. VIGANÒ), Torino, 2015, p. 71 ss.

¹⁴³ L'insieme di dati e contenuti è reso internazionalmente invisibile e non accessibile dai comuni browser. Infatti, per potervi accedere è necessario il possesso di *software* per la comunicazione anonima.

¹⁴⁴ Per un approfondimento, W. LACSON, B. JONES, *The 21st Century DarkNet Market: Lessons from the Fall of Silk Road*, in *International Journal of Cyber Criminology*, 1, 2016, p. 40 ss.

¹⁴⁵ Così, A. WANG, *Silk Road: The "eBay" for Narcotics*, in *The Epoch Times*, 6 giugno 2011. Per un approfondimento, T. SWIFT, *What is the 'Deep Web'? And Other Questions About the Shadowy Virtual World of Silk Road*, in *Baltimore Sun Online*, 3 ottobre 2013, <http://www.baltimoresun.com/business/technology/blog/bal-silk-road-deep-web-explainer20131003-story.html>; N. BURLEIGH, *The Rise and Fall of Silk Road, the Dark Web's Amazon*, in *Newsweek*, 19 febbraio 2015, <http://www.newsweek.com/2015/02/27/silk-road-hell307732.html>. In generale, v., United States v. Ulbricht, 79 F. Supp. 3d 466 (S.D.N.Y. 2015).

¹⁴⁶ Cfr., *Ergastolo per il fondatore di Silk Road, mercato nero del web*, in *La Repubblica*, 30 maggio 2015.

¹⁴⁷ Si trattava di un market digitale da oltre centomila annunci. Nel corso dell'operazione, Darknet.Drug, la Guardia di Finanza ha sequestrato anche 2,2 kg di sostanze stupefacenti, tra cui cocaina, ketamina e Mdma, nonché 163 pasticche di ecstasy e 78 francobolli impregnati di Lsd. Sequestrato anche un locale commerciale in cui si potevano convertire valute correnti con i Bitcoin.

Secondo la Guardia di Finanza si trattava del «più importante mercato del dark web». Circa 30mila annunci erano riservati a farmaci e sostanze stupefacenti, tra cui psicofarmaci, cannabis, oppioidi, steroidi, cocaina e eroina. Tutto ordinatamente suddiviso in categorie.

Ma sul Berlusconi Market trovavano spazio anche annunci di gioielli, che le Fiamme Gialle sospettano rubati o contraffatti, nonché armi. Circa 5mila annunci si riferivano a pistole, fucili, esplosivi e munizioni. Fra gli articoli in vendita anche *malware* e *botnet*, utili per attacchi informatici.

Esattamente come nel film *Point Break* di Kathryn Bigelow, ai gestori del Berlusconi Market piaceva camuffare le proprie identità dietro quelle di politici famosi. Cfr., V. BERRA, *Armi, droga e malware. Tutto quello che potevate trovare nel "Berlusconi Market", il negozio "più affidabile" del dark web*, in *Open.online*, 7 novembre 2019, <https://www.open.online/2019/11/07/operazione-darknet-la-guardia-di-finanza-chiude-il-market-piu-affidabile-del-dark-web/>. Per un ulteriore approfondimento, si visiti il sito

(non vi è alcun tipo di collegamento con la più famosa famiglia lombarda). Dopo le operazioni dell'FBI statunitense e della polizia olandese nei confronti dei *Black Market* "Silk Road", "Alfa Bay" e "Hansa Market", Berlusconi Market costituisce uno dei più importanti esempi al mondo di *Black Market* del *Dark Web* reso non più operativo.

Inoltre, dopo aver scoperto una chat, la *Shoah Party*, in cui dei ragazzini si scambiavano video e foto pedofili e inneggianti al nazismo, è stata disposta la chiusura di siti nel *dark web* che diffondevano e detenevano materiale pedo-pornografico ceduto dietro compenso in *bitcoin*, o ove si consumavano torture in diretta su minori, poi uccisi¹⁴⁸. Questi sono solo alcuni esempi di condotte tenute nel *dark web* e che spesso passano inosservate, perché i reati sono commessi in un ambiente occulto e segreto.

In un simile contesto, caratterizzato da una evidente fluidità, transnazionalità e velocità delle operazioni, è fondamentale la cooperazione tra Stati, in particolar modo tra organi di polizia ed autorità giudiziarie. Ciò anche alla luce dell'incrementato numero nel *dark web* di negozi *online* con un solo fornitore e mercati più piccoli e frammentati su *Tor*, compresi quelli in specifiche lingue. Alcuni gruppi criminali organizzati stanno anche frammentando le loro attività in una serie di siti e mercati *online* con pseudonimi, presentando quindi ulteriori sfide per l'applicazione della legge¹⁴⁹.

Una delle iniziative avviate da Europol è quella di creare un coordinamento nell'applicazione della legge per contrastare la criminalità nel *dark web* con la partecipazione di forze dell'ordine di tutti gli Stati membri dell'UE, terze parti operative e altri partner pertinenti, come Eurojust. Per raggiungere questo obiettivo, Europol ha istituito un *Dark Web Team* dedicato alla collaborazione con i partner dell'UE e con le forze dell'ordine in tutto il mondo al fine di ridurre le dimensioni di queste forme di criminalità. Il team ha il compito di condividere informazioni; fornire supporto operativo e competenza in diverse aree criminali; sviluppare strumenti, tattiche e tecniche per condurre indagini sul *dark web*; identificare minacce e obiettivi. Il team mira inoltre a rafforzare azioni tecniche e investigative congiunte, organizzare iniziative di formazione e rafforzamento delle capacità, insieme a campagne di prevenzione e sensibilizzazione, attuando una vera e propria strategia a 360 gradi contro la criminalità nel *dark web*.

Proprio grazie a tale interazione, sono stati abbattuti due prolifici mercati del *dark web* in operazioni globali simultanee, supportate da Europol: il *Wall Street Market* e il *Silkkitie* (noto come il *Valhalla Marketplace*)¹⁵⁰. Le operazioni sono state svolte dalla polizia

della Guardia di finanza: <http://www.gdf.gov.it/stampa/ultime-notizie/anno-2019/novembre/arrestati-tre-amministratori-del-black-market-denominato-berlusconi-market-attivo-nel-dark-web>.

¹⁴⁸ In questi siti circolavano immagini di efferata violenza, anche in situazioni 'live', in cui agli utenti che riuscivano ad accedere a questi ambienti reconditi veniva consentito di interagire in condotte di violenza sessuale e tortura su minori, attuate in diretta da adulti. Cfr., *Pedopornografia, sevizie in diretta sul "dark web" dietro pagamento di Bitcoin: indagati due 17enni piemontesi*, in *Il fatto quotidiano*, 15 luglio 2020, consultabile al link: <https://www.ilfattoquotidiano.it/2020/07/15/pedopornografia-sevizie-in-diretta-sul-dark-web-dietro-pagamento-di-bitcoin-indagati-due-17enni-piemontesi/5868789/>; L. SERRANÒ, "Torture e violenze sessuali in diretta sui minori nel dark web": lo scoprono i carabinieri di Siena, in *La Repubblica*, 15 luglio 2020, consultabile al link: https://firenze.repubblica.it/cronaca/2020/07/15/news/torture_e_violenze_sessuali_in_diretta_sui_minori_nel_dark_web_lo_scoprono_i_carabinieri_di_siena-261976327/.

¹⁴⁹ Cfr., EUROPEAN POLICE OFFICE (EUROPOL), *The Internet Organised Crime Threat Assessment (IOCTA) 2019*, The Hague, 2019, disponibile al link: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019>.

¹⁵⁰ Il *Wall Street Market* era il secondo mercato illegale online al mondo nel *dark web*. I responsabili del sito furono arrestati in Germania e due dei fornitori di stupefacenti più venduti furono arrestati negli Stati Uniti. Le autorità finlandesi, invece, hanno chiuso *Silkkitie*, mentre contestualmente le autorità

criminale federale tedesca (Bundeskriminalamt), la quale ha chiuso il *Wall Street Market*, sotto l'autorità della procura tedesca. La polizia tedesca è stata supportata dalla polizia nazionale olandese (*Politie*), Europol, Eurojust e varie agenzie governative statunitensi (*Drug Enforcement Administration, Federal Bureau of Investigation, Internal Revenue Service, Investments Security Homeland, Investigations Security degli Stati Uniti, US Postal Inspection Service e US Department of Justice*). La *Silkkitie* (nota come il *Valhalla Marketplace*) e il suo contenuto sono stati sequestrati anche dalla dogana finlandese (*Tulli*) in stretta collaborazione con la polizia nazionale francese (*La Police Nationale Française*) ed Europol. Europol è stato assistito da *Bitdefender*, una società di sicurezza Internet che fornisce consulenza al Centro europeo per la criminalità informatica (EC3).

È evidente, allora, la necessità di un coordinamento investigativo e di polizia al fine di combattere efficacemente la criminalità *online*. Il crimine, infatti, si diffonde nel nuovo mondo informatico, creandosi nuovi spazi d'azione, ed arrivando sino a ricorrere alla comunicazione informatica mediante *social network*.

Innanzitutto a tale situazione, anche le tecniche investigative devono affinarsi ed essere al passo con i tempi. Vi è, dunque, la necessità che le nuove tecnologie informatiche diventino strumento utile nelle mani degli investigatori, al fine di combattere la criminalità cibernetica che, grazie alla digitalizzazione imperante, sfrutta in modo prevalente nuovi mezzi, anche di comunicazione.

Il successo di queste operazioni fa contare sul fatto che si stia avviando una stagione caratterizzata da centinaia di nuove indagini in Europa condotte nel *cyberspace*¹⁵¹. Ne sono una dimostrazione proprio queste due grosse operazioni di contrasto, guidate dall'FBI, dalla DEA e dalla polizia nazionale olandese, col sostegno di Europol¹⁵². Essa, coordinata nell'UE e negli USA, si colloca fra le più sofisticate azioni di smantellamento nella lotta contro le attività criminali *online*.

Questa opinione sarebbe suffragata anche da alcune risoluzioni del Parlamento europeo, con le quali: ha incoraggiato la rete INHOPE a lavorare con i suoi membri per creare un meccanismo di segnalazione anonimo e sicuro sulle reti *Deep Web*, ad esempio le reti *Dark Net* che si trovano nella rete TOR, che garantisca lo stesso standard elevato di anonimato offerto dagli organi di stampa agli informatori, per offrire la possibilità a coloro che utilizzano tali reti di fornire informazioni o segnalazioni sul materiale contenente abusi sessuali su minori; ha invitato gli Stati membri ad attuare pienamente la direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile; ha esortato le autorità preposte all'applicazione della legge, sia a livello nazionale che dell'UE, a investire nelle nuove tecnologie per lottare contro i reati nel «*dark web*» e nel «*deep web*»; ha sottolineato che Eurojust ed Europol devono ricevere le risorse adeguate per migliorare l'identificazione delle vittime, per lottare contro le reti organizzate di autori di reati di abuso sessuale e per accelerare il rilevamento, l'analisi e la segnalazione di materiale pedopornografico *online* e *offline*¹⁵³.

tedesche hanno posto fine alle loro attività illegali nel momento in cui gli stessi trafficanti hanno trasferito le loro attività in un altro sito commerciale illegale su Tor.

¹⁵¹ Per un contributo di carattere introduttivo relativo alla cooperazione internazionale nel *cyberspace* e ai possibili scenari futuri, P. PAWLAK, A. MISSIROLI, *Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace*, in *European Foreign Affairs Review*, 2, 2019, pp. 125-134.

¹⁵² Le operazioni hanno portato alla chiusura dell'infrastruttura di un'economia criminale sommersa responsabile del commercio di più di 350.000 prodotti illegali, fra cui droga, armi da fuoco e malware di criminalità informatica.

¹⁵³ Cfr., Risoluzione del Parlamento europeo del 14 dicembre 2017 sull'attuazione della direttiva 2011/93/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso

A ben vedere, senza voler scomodare il *dark web*, il crimine ha sviluppato nuove modalità per garantire il proprio anonimato in rete ed al tempo stesso ampliare la platea di possibili persone offese che navigano nel *surface web*. Esistono, infatti, altre modalità tecniche, che offrono però una minor tutela. Si pensi ad esempio alla creazione di *account e-mail* con dati identificativi falsi, o all'apertura di profili *social* utilizzando pseudonimi o false generalità. Spesso si sfocia in vere e proprie identità virtuali, spesso plurime. Grazie a queste tecniche simulatorie, il criminale riesce ad ottenere una vera e propria maschera, diventando nella rete «uno, nessuno, centomila» e riuscendo a consumare estorsioni a danno di vittime ignare di intrattenere conversazioni con persone che appaiono quelle che in realtà non sono. È così, ad esempio, che il «signor Nessuno» può agire creando anche molteplici identità, mediante profili *fake* su *Facebook*, volti a nascondere i veri dati anagrafici, e finalizzati alla consumazione dei reati¹⁵⁴.

3.4. Il cloud computing

Ulteriore strumento utilizzato dalla criminalità informatica per diffondere nel *cyberspazio* materiale illecito e consumare reati disperdendo le proprie tracce è il *cloud computing*¹⁵⁵. Si tratta di uno spazio virtuale detto “nuvola”¹⁵⁶ o “spazio informatico” che costituisce un enorme serbatoio¹⁵⁷, dalle imponenti potenzialità per aziende e privati che vogliono conservare i propri dati in uno spazio virtuale sempre accessibile da qualsiasi luogo fisico e con qualsiasi dispositivo in grado di collegarsi ad *internet*.

Il *cloud computing* è un sistema di elaborazione distribuito e basato su *internet*¹⁵⁸. È possibile ritenere il *cloud* «un insieme di servizi offerti da un provider, che permettono di

e lo sfruttamento sessuale dei minori e la pornografia minorile (2015/2129(INI)), (2018/C 369/13); Risoluzione del Parlamento europeo del 13 dicembre 2016 sulla situazione dei diritti fondamentali nell'Unione europea nel 2015 (2016/2009(INI)), (2018/C 238/01).

¹⁵⁴ Per l'analisi di un caso concreto, sia consentito il rinvio ad A. GAUDIERI, *Estorsione via chat e gravi indizi di colpevolezza nel procedimento penale*, cit., p. 137 ss. Più in generale, sul tema, U. BARDARI, *Le identità nei social network: strumenti tecnici virtuali con conseguenze giuridiche reali*, in AA.VV., *Questioni di informatica forense* (a cura di C. MAIOLI), Roma, 2015, p. 151 ss.; M. GEROSA, *Second Life*, Milano, 2007; A. GRANELLI, *Il sé digitale*, Milano, 2006; M. REDOLFI, *Anonimato in rete: note tecniche*, in AA.VV., *Sicurezza e anonimato in rete* (a cura di A. MAGGIPINTI, M. IASELLI), Milano, 2005, p. 34; S. TURKLE, *La vita sullo schermo. Nuove identità e relazioni sociali nell'epoca di Internet*, Milano, 1997; G. VACIAGO, *Internet e crimini informatici*, in AA.VV., *Computer Crimes. Casi pratici e metodologie investigative dei reati informatici* (a cura di M.L. PICCINNI, G. VACIAGO), Bergamo, 2008, p. 12 ss.

¹⁵⁵ Per gli aspetti strettamente tecnici, si rinvia a S. MURUSEGAN, I. BOJANOVA (a cura di), *Encyclopedia of Cloud Computing*, Hoboken, 2016; B. FURHT, A. ESCALANTE (a cura di), *Handbook of Cloud Computing*, New York, Dordrecht, Heidelberg, London, 2010.

¹⁵⁶ Si riferisce al simbolo della nube, generalmente impiegato nei diagrammi tecnici per rappresentare graficamente le connessioni telematiche tra più elaboratori. In argomento, NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, *The NIST Definition of Cloud Computing*, 2011, p. 6, consultabile all'indirizzo <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>, ove si legge che «Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models».

¹⁵⁷ Si pensi ai supporti di memoria virtuali quali dropbox, google drive, onedrive, icloud, ecc.

¹⁵⁸ In merito alle specifiche iniziative assunte dall'Unione europea relative al *cloud*: Conclusioni del Consiglio sul tema «*Plasmare il futuro digitale dell'Europa*» (2020/C 202 I/01); Comunicazione della Commissione «*Una strategia europea per i dati*» (COM(2020) 66 final); Comunicazione della Commissione «*Iniziativa europea per il cloud computing - Costruire un'economia competitiva dei dati e*

memorizzare, archiviare ed elaborare grandi quantità di dati e di informazioni grazie all'utilizzo di risorse *hardware* e *software* disponibili in rete» consistente in un «nuovo modo di organizzare e rendere fruibili tecnologie esistenti, integrandone le componenti e presentando all'utente solo le funzioni d'uso»¹⁵⁹. Si pensi ad un grande computer realizzato da un insieme di sistemi elettronici connessi tra loro attraverso *internet* e quindi mediante una connessione telematica, non individuabile in un determinato luogo¹⁶⁰.

Evidenti sono i vantaggi dell'impiego del *cloud*: consente di disporre di dati «ubiqui», cioè accessibili da qualunque luogo e da qualunque dispositivo; garantisce l'anonimato; fornisce servizi gratuiti o a basso costo¹⁶¹; i costi di gestione e manutenzione gravano sui fornitori del servizio; assicura l'interazione tra dispositivi informatici; fornisce spazi per la conservazione dei dati dalla capienza pressoché infinita; consente soluzioni flessibili di allocazione delle risorse, adattandosi di continuo alle esigenze dell'utente¹⁶².

La natura e la struttura tecnica dello strumento si presta però a scopi illeciti. Anche in questo caso, è stata avviata una incessante ed imperitura lotta tra utilizzo criminoso delle tecniche informatiche e investigazioni altamente specializzate, ove le forze dell'ordine e la magistratura tentano – impiegando tutte le risorse messe a loro disposizione – di stare al passo coi criminali mediante strumenti tecnologici spesso *borderline* relativamente alle garanzie previste dalla legge e che sfruttano talvolta mezzi tanto invasivi della riservatezza quanto quelli utilizzati dagli *hackers*.

I dati contenuti in un *cloud* possono essere obiettivo privilegiato per la criminalità informatica. Inoltre, va rammentato che tali dati non sono collocati in un luogo fisico, ma in una sfera territoriale totalmente ideale¹⁶³.

della conoscenza in Europa” (COM(2016)0178); Comunicazione della Commissione “Strategia per il mercato unico digitale in Europa” (COM(2015)0192); Comunicazione della Commissione “Verso una florida economia basata sui dati” (COM(2014)0442); Comunicazione della Commissione “Un'industria europea più forte per la crescita e la ripresa economica” (COM(2012)0582); Comunicazione della Commissione “Sfruttare il potenziale del cloud computing in Europa” (COM(2012)0529 final); Comunicazione della Commissione “Calcolo ad alte prestazioni: il posto dell'Europa nella corsa mondiale” (COM(2012)0045). Cfr., anche, AGENZIA PER L'ITALIA DIGITALE, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, in www.archivio.digitpa.gov.it, 2012.

¹⁵⁹ Così, F. BASSANINI, E. BELLONI, *L'impatto del cloud computing sull'economia italiana*, Roma, 2011, p. 12 ss. V., anche, sul tema S. ATERNO, voce Digital forensics (*investigazioni informatiche*), in *Dig. disc. pen.*, Agg. VIII, Torino, 2014, p. 217 ss.; S. ATERNO, M. MATTIUCCI, *Cloud Forensic e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.*, 3, 2013, pp. 865-878; V. BERLINGÒ, *Il fenomeno della datafication e la sua giuridicizzazione*, in *Riv. trim. dir. pubbl.*, 3, 2017, p. 641. Similmente, G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021, p. 87, ove l'A. parla di un «complesso di strumenti tecnici attraverso i quali un utente elabora, usa e archivia, per il tramite di Internet, dati contenuti su computer remoti, cioè da questi non fisicamente raggiungibili, sfruttandone le potenzialità di calcolo e memorizzazione».

¹⁶⁰ S. ATERNO, *Cloud forensics: aspetti giuridici e tecnici*, in A.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1690

¹⁶¹ I servizi possono essere offerti congiuntamente da un medesimo operatore o, come spesso accade, da diversi *providers* che operano attraverso “*contractual chains*”. Si veda, a proposito, W.K. HON, C. MILLARD, I. WALDEN, *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*, in *Stanford Technology Law Review*, 2012, p. 83, i quali osservano come «Several entities may be involved in providing a single cloud service, including suppliers of hardware, software, and data center services. There may be chains of contracts between them. Contractual requirements may vary with the cloud “stack” component under consideration». Sul punto, anche, V. FALCE, *Standard e Cloud computing*, in *Il diritto industriale*, 2 2015, p. 155.

¹⁶² Sul punto, S. ATERNO, *Cloud forensics: aspetti giuridici e tecnici*, cit., p. 1689; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 37.

¹⁶³ In proposito, le criticità relative all'individuazione del luogo in cui si trovano i dati derivano dal fatto che «la tecnologia *cloud* ottimizza le risorse informatiche mediante la c.d. ridondanza o *load*

Com'è facilmente intuibile, dal punto di vista giuridico, un primo problema che si pone è relativo al luogo fisico in cui allocare il *cloud*. La questione non è di poco conto perché intorno ad essa ruotano una serie di problematiche relative all'individuazione della giurisdizione, della competenza del giudice ed il rispetto del principio del giudice naturale precostituito per legge. Ulteriori problematiche, poi, coinvolgono il rispetto dei principi e delle regole disposte in tema di prova. Le incertezze poste alla base del *cloud* rendono l'argomento particolarmente dibattuto nell'ambito della *forensics*.

Un esempio per far comprendere la portata del fenomeno è il seguente: il *cloud*, in quanto sistema altamente dinamico ed autoriconfigurabile, è in grado di far fronte a qualsiasi richiesta proveniente da qualsiasi parte del globo terrestre. Questo comporta che se un server, nel momento in cui parte la richiesta di un utente, è particolarmente occupato e non risponde, un altro server appartenente allo stesso spazio informatico, virtuale ed ideale, prenderebbe prontamente il suo posto, rispondendo alla richiesta, in modo da evitare che all'utente non sia garantito il servizio¹⁶⁴. È evidente, allora, che – in caso di consumazione di reati – si pongano problematiche relative al luogo ed ai soggetti coinvolti, inclusi gli *Internet Service Provider*.

Ed invero, la massiccia diffusione dei servizi di *cloud computing* forniti dagli *Internet Service Provider* ha determinato quella che viene solitamente definita come *loss of location* del dato digitale, la quale rende particolarmente complessa l'individuazione dello Stato a cui rivolgere la richiesta di assistenza giudiziaria, poiché il luogo in cui sono conservati i dati è mobile e in continuo movimento¹⁶⁵. Ciò, ovviamente, ha effetti negativi anche sulla cooperazione giudiziaria internazionale, sullo svolgimento delle indagini transfrontaliere ed in particolare sulle regole relative alla formazione della prova digitale, indipendentemente da luogo di conservazione dei dati.

In questa direzione vanno le iniziative intraprese dal Consiglio d'Europa e dell'Unione europea, le quali stanno regolamentando la cooperazione diretta tra inquirenti e *Internet Service Provider*, mediante un "ripensamento" del classico schema basato sul principio del mutuo riconoscimento ed indipendentemente dal luogo in cui i dati informatici sono conservati: il secondo Protocollo alla Convenzione di Budapest e la proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali, nonché la proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

Infine, il Consiglio europeo ha sottolineato la necessità di istituire servizi *cloud* europei affidabili, sicuri e protetti, al fine di garantire che i dati europei possano essere conservati e trattati in Europa, nel rispetto delle norme e delle regole europee. Pertanto, ha sviluppato il concetto di un'infrastruttura cloud federata dell'UE e ha invitato la Commissione a portare avanti i relativi lavori con celerità. Una maggiore capacità di *cloud* a livello europeo, insieme a un quadro di interoperabilità abilitante, dovrebbe inoltre consentire la diffusione di soluzioni digitali pubbliche e private basate su *cloud*

balancing, grazie alla quale i dati possono essere spostati automaticamente, e pure per brevi periodi di tempo, da un *server* all'altro, anche se questi ultimi sono localizzati in Stati diversi». In questi termini, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 37 ss.

¹⁶⁴ Cfr., S. ATERNO, *Cloud forensics: aspetti giuridici e tecnici*, cit., p. 1690.

¹⁶⁵ Così, F. GRAZIANI, *La ricerca della prova digitale mediante captatore informatico nella prassi degli Stati e nell'ordinamento italiano: il difficile equilibrio tra prevenzione dei reati e tutela della riservatezza informatica*, cit., p. 397.

sicure e protette che garantiscano, tra l'altro, un accesso più rapido e più efficace, pratico e trasparente ai servizi di *e-gouvernement*¹⁶⁶.

4. Argomentazioni sul *locus commissi delicti*. La difficile applicazione dei criteri di giurisdizione e di competenza del giudice

Come precedentemente illustrato, il *cyberspace* è un dominio di difficile regolamentazione. Nello specifico, la complessa struttura di questo spazio ha reso particolarmente contorta la regolamentazione della giurisdizione e della competenza del giudice. A conferma di quanto appena affermato militano le tante fonti – spesso non coordinate tra loro – che tentano di rispondere all'esigenza di rispettare il supremo principio del giudice naturale precostituito per legge¹⁶⁷, ma che tradiscono un evidente, vivo ed attuale pericolo di lesione di tale diritto fondamentale.

Il rispetto delle regole sulla competenza territoriale va ricondotto al principio del giudice naturale: «qualsiasi istituto processuale, quindi, che producesse [...] l'effetto di “distrarre” il processo dalla sua sede, inciderebbe su un valore di elevato e specifico risalto per il processo penale; giacché la celebrazione di quel processo in “quel” luogo, risponde ad esigenze di indubbio rilievo, fra le quali, non ultima, va annoverata anche quella [...] per la quale il diritto e la giustizia devono riaffermarsi proprio nel luogo in cui sono stati violati»¹⁶⁸. Infatti, nel processo penale «il predicato della “naturalità” assume

¹⁶⁶ Cfr., Conclusioni del Consiglio europeo del 1° e 2 ottobre 2020, EUCO 13/20.

¹⁶⁷ Va chiarito che la naturalità del giudice non può ridursi a mero riferimento alla competenza per territorio, nonostante storicamente i due concetti vengano accostati, altrimenti si finirebbe per appiattare la definizione di naturalità su quella di precostituzione. Così interpretato, l'art. 25 Cost. conterrebbe unaendiadi costituita dai termini “naturale” e “precostituito”. La dottrina riconosce nel giudice naturale quello che l'ordinamento considera più idoneo ad accertare il fatto di reato nel rispetto della legge e dei diritti dell'imputato, nell'esercizio delle proprie funzioni, dimostrando in concreto di possedere tutte le prerogative di *status* e i presupposti per esser ritenuto tale. Il giudice naturale in possesso di tali requisiti è colui il quale è sottoposto al controllo dei suoi spettatori naturali, quali la collettività coinvolta più da vicino dal reato. In tale contesto, la naturalità attribuirebbe al giudice la qualità di accertare, prima di ogni altro, se un precetto è stato violato e a riaffermarne il valore, con la condanna e la punizione di chi vi ha trasgredito. Sul punto, A.A. DALIA-FERRAIOLI, *Manuale di diritto processuale penale*, Padova, 2018, p. 92 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 81 ss. L'A. chiarisce che vi sono casi in cui l'interesse a che il processo si svolga in quella determinata sede davanti al suo pubblico, secondo la regola del *locus commissi delicti*, cede innanzi ad interessi superiori, pur essi prestabiliti, poiché risulta lesa, ad esempio, l'imparzialità del giudice. È il caso dell'intero ufficio giudiziario che appare parziale o esposto a pressioni ambientali; oppure il caso dell'organo giudicante che debba decidere su di un magistrato che svolga le sue funzioni in quel distretto e che sia imputato, persona offesa o danneggiato dal reato.

¹⁶⁸ Così, Corte Cost., sentenza del 21 aprile 2006, n. 168; Corte Cost., sentenza del 27 febbraio 2018. Per un commento a tale ultima sentenza, E. APRILE, *Osservazioni a C. Cost, data udienza (21 febbraio 2018), data deposito 27 aprile 2018, n. 92*, in *Cass. pen.*, 7-8, 2018, p. 2450b ss.; L. ALGERI, *L'esame del minore al vaglio della Consulta: la mobilità del giudice naturale preserva la concentrazione*, in *Dir. pen. proc.*, 12, 2018, p. 1565 ss.; C. GABRIELLI, *Costituzionalmente legittima la disciplina dell'ascolto protetto del minore: un approdo condivisibile, al di là di qualche ambiguità argomentativa*, in *Giurisprudenza costituzionale*, 2, 2018, p. 815C ss.; ID., *La disciplina dell'esame del minore in incidente probatorio regge alle censure di incostituzionalità*, in *Riv. it. Dir. e proc. pen.*, 2, 2018, p. 964 ss.; S. RECCHIONE, *Estensione delle rogatorie per l'assunzione della testimonianza del minore: la Corte Costituzionale dichiara infondata la questione, già sussistendo le garanzie invocate dal rimettente*, in *Dir. pen. cont.*, 5, 2018, p. 309. Sia, inoltre, consentito il rinvio ad A. GAUDIERI, *Corte cost., 21 febbraio – 27 aprile 2018, n. 92*, in AA.VV., *Corte costituzionale e sistema processuale penale. L'elaborazione giurisprudenziale del 2018* (a cura di D. CIMADOMO, G. DALIA), Milano, 2019, p. 143 ss.

[...] un carattere del tutto particolare, in ragione della “fisiologica” allocazione di quel processo nel *locus commissi delicti*»¹⁶⁹.

Il problema non è di poco conto, perché il rispetto delle regole poste a garanzia del diritto ad un giudice precostituito coinvolge tutti gli aspetti processuali, incluso – ed a maggior ragione – quelli relativi alla corretta formazione della prova, basato su un *iter* che parte dalla ricerca e prosegue con l’ammissione, l’assunzione e la valutazione. A ciò si aggiungano i perduranti dubbi relativi ad aspetti della cooperazione giudiziaria in materia penale non regolamentati o regolamentati nebulosamente, ed alla carente legislazione in tema di informazioni e prove informatiche. Non vanno infine trascurate le possibili ricadute negative sul piano della qualità dell’accertamento: in assenza di regole specifiche per il settore, alcune fonti di prova rilevanti potrebbero risultare indisponibili o difficilmente reperibili.

¹⁶⁹ Corte Cost., sentenza del 21 aprile 2006, n. 168. Tale sede giudiziaria è ritenuta, in linea di massima, anche quella più idonea all’accertamento del fatto, al fine di una più agevole e rapida raccolta del materiale probatorio, nonché di un pieno rispetto del diritto di difesa. Per la Consulta è evidente che le norme sulla competenza territoriale siano attuative del principio del “giudice naturale”.

Per un vasto approfondimento sul principio del giudice naturale, nell’ampia letteratura, M. ALFIERI, *Giudice naturale*, in *Dig. disc. pen.*, V, Torino, 1991, p. 442 ss.; G. CONSO, *Il principio della certezza del giudice ed i limiti che lo condizionano*, in AA.VV., *Costituzione e processo penale* (a cura di G. CONSO), Milano, 1969, p. 418 ss.; ID., *Validità costituzionale della rimessione per motivi d’ordine pubblico o per legittimo sospetto*, in AA.VV., *Costituzione e processo penale* (a cura di CONSO), Milano, 1969, p. 432 ss.; F. CORDERO, *Connessione e giudice naturale*, in AA.VV., *Connessione di procedimenti e conflitti di competenza* (Atti del Convegno di studio svoltosi a Trieste-Grignano, 3-5 ottobre 1975), Milano, 1976, p. 53; A.A. DALIA, *Sulla precostituzione del giudice naturale come fondamentale garanzia di certezza per l’imputato, con particolare riguardo ai rapporti tra la competenza penale dei consoli e dei comandanti di porto*, in *Riv. it. dir. e proc. pen.*, 1965, p. 507; P. DE LALLA, *La scelta del rito istruttorio*, Napoli, 1971, p. 74 ss.; DE LISO, “Naturalità” e “precostituzione” del giudice nell’art. 25 della Costituzione, in *Giur. Cost.*, 1969, p. 2671 ss.; A. DIDI, *La rimessione del processo penale*, Milano, 2000, p. 133; G. FOSCHINI, *Giudice naturale e costituzione del giudice*, in G. FOSCHINI, *Tornare alla giurisdizione. Saggi critici*, Milano, 1971, p. 81 ss.; E.T. LIEBMAN, *Giudice naturale e costituzione del giudice*, in *Riv. dir. proc.*, 1964, p. 331 ss.; P. MOSCARINI, *Naturalità e imparzialità del giudice*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale. Salerno, 25-27 ottobre 2018* (a cura di L. KALB), Milano, 2019, p. 291 ss.; M. NOBILI, sub *Art. 25 comma 1 Cost.*, in AA.VV., *Commentario della Costituzione* (a cura di G. BRANCA, A. PIZZORUSSO), Bologna, 2004, p. 135 ss.; A. PINTO, *Giudice naturale e legittima suspicio*, in *Riv. pen.*, 1967, p. 133 ss.; M. PISANI, *La garanzia del “giudice naturale” nella Costituzione italiana*, in *Riv. it. dir. e proc. pen.*, 1961, p. 414 ss.; A. PIZZORUSSO, *Giudice naturale*, in *Enc. giu. Treccani*, XVI, Roma, 1989, p. 1 ss.; R. ROMBOLI, *Il giudice naturale. I. Studio sul significato e la portata del principio nell’ordinamento costituzionale italiano*, Milano, 1981; G. SABATINI, *La competenza surrogatoria ed il principio del giudice naturale nel processo penale*, in *Riv. it. dir. e proc. pen.*, 1962, p. 941 ss.; E. SOMMA, “Naturalità” e “precostituzione” del giudice nell’evoluzione del concetto di legge, in *Riv. it. dir. e proc. pen.*, 1963, p. 797 ss.; G. SPANGHER, *La rimessione dei procedimenti*, I, *Precedenti storici e profili di legittimità costituzionale*, Milano, 1984, p. 286; C. TAORMINA, *Giudice naturale e processo penale*, Roma, 1972, p. 168 ss.; G. UBERTIS, “Naturalità” del giudice e valori socio-culturali nella giurisdizione, in *Riv. it. dir. e proc. pen.*, 1977, p. 1058 ss.; ID., “Naturalità” e “precostituzione” del giudice nell’evoluzione del concetto di legge, in *Riv. it. dir. e proc. pen.*, 1963, p. 943 ss.; F. ZACCHÈ, sub *Art. 25 Cost.*, in AA.VV., *Codice di procedura penale commentato* (a cura di A. GIARDA, G. SPANGHER), tomo I, Milanofiori Assago, 2017, p. 51 ss.; G. ZAGREBELSKY, *Connessione e giudice naturale*, in AA.VV., *Connessione di procedimenti e conflitti di competenza* (Atti del Convegno di studio svoltosi a Trieste-Grignano, 3-5 ottobre 1975), Milano, 1976, p. 59 ss.; N. ZANON, F. BIONDI, *Il sistema costituzionale della magistratura*, Bologna, 2006, p. 113 ss. Per un’importante analisi del principio del giudice naturale nei casi di competenza per connessione, L. KALB, *Il processo per le imputazioni connesse*, Torino, 1990, in particolare v. capitolo IV, *Giudice naturale e competenza per connessione*, p. 129 ss.

È evidente che una legislazione basata su luoghi fisici, formatasi in un periodo storico in cui le questioni relative al mondo digitale erano statisticamente irrilevanti e comunque limitate, non può oggi – se non attraverso una giurisprudenza innovativa – rispondere alle esigenze poste da un tema ormai diventato scottante e di quotidiana discussione tra gli addetti ai lavori.

Si vuole, perciò, da subito inusualmente anticipare la conclusione. Il rischio che si lasci alla giurisprudenza il compito di individuare – attraverso un’interpretazione spesso creativa di principi illogici ed asistematici – una soluzione rispetto a casi concreti che difficilmente sembrano risolvibili con il sistema normativo vigente, potrebbe comportare, in futuro, una seria lesione del principio di legalità e, in particolare, del principio del giudice naturale precostituito per legge per le ragioni di seguito esposte.

A ciò si arriva mediante un’analisi critica e sistematica delle fonti attualmente in vigore e della relativa giurisprudenza formatasi, che ha dovuto adattarsi alla normativa esistente (o assente).

Com’è noto, l’ambito spaziale di obbligatorietà della legge penale individua i confini della giurisdizione penale¹⁷⁰, in particolare quando i reati presentino elementi di extranazionalità.

In tema, è fondamentale anche comprendere quali siano le regole da rispettare al fine di individuare il giudice competente per territorio¹⁷¹ e se queste, ad oggi, subiscano una “torsione applicativa” rispetto a quanto voluto dai padri del codice repubblicano, di stampo tendenzialmente accusatorio. Inoltre, ha una particolare importanza anche per stabilire l’ambito di operatività delle regole relative al trasferimento dei procedimenti penali¹⁷². Di ausilio potrebbe risultare la normativa e la giurisprudenza internazionale e sovranazionale¹⁷³.

L’art. 22 della Convenzione del Consiglio d’Europa sulla criminalità informatica¹⁷⁴ prevede che ogni Parte deve adottare le misure necessarie per stabilire la propria competenza – *rectius*, giurisdizione – per tutti i reati previsti in conformità agli articoli da

¹⁷⁰ Per giurisdizione si intende la funzione dello Stato consistente nell’applicazione della legge al caso concreto con forza cogente da parte di un giudice terzo ed imparziale. Sulla giurisdizione, con particolare riferimento al diritto penale internazionale, I. CARACCILO, *Dal diritto penale internazionale al diritto internazionale penale*, Napoli, 2000, *passim*.

¹⁷¹ La competenza è quella fetta di funzione giurisdizionale che la legge assegna al singolo giudice, in ragione della necessità di predeterminare, in relazione ad ogni fatto penalmente rilevante, l’organo che, in concreto, risulti legittimato a prendere la cognizione. I criteri di competenza sono quattro: tre di natura codicistica (materia, territorio e connessione) ed uno di creazione dottrina (funzione).

¹⁷² Sul trasferimento dei procedimenti penali stranieri, L. KALB, sub *Art. 746 bis – 746 quater c.p.p.*, in AA.VV., *Commentario breve al codice di procedura penale* (a cura di G. ILLUMINATI, L. GIULIANI), Milano, 2020, p. 3571 ss.

¹⁷³ Si attestano sei criteri per individuare la giurisdizione penale nel contesto internazionale: il criterio di territorialità, il principio della nazionalità attiva, il principio della nazionalità passiva, il criterio della bandiera, il principio di universalità, il principio del Paese titolare dell’interesse leso. Per un approfondimento, G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, cit., p. 92 ss.

¹⁷⁴ La Convenzione del Consiglio d’Europa sulla criminalità informatica è stata firmata a Budapest il 23 novembre 2001 ed è entrata in vigore il 1° luglio 2004, ossia il primo giorno del mese successivo alla scadenza dei tre mesi successivi alla data in cui cinque Stati, compresi almeno tre Stati membri del Consiglio d’Europa, hanno espresso il loro consenso ad essere vincolati dalla Convenzione. Rappresenta il primo trattato internazionale sulle infrazioni penali commesse via internet e su altre reti informatiche. Contiene inoltre una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l’intercettazione dei dati. Obiettivo principale, così come enunciato nel preambolo, è quello di perseguire una politica penale comune per la protezione della società contro la cibercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

2 a 11 della Convenzione, quando i reati siano commessi: a. nel proprio territorio; b. a bordo di una nave battente bandiera della Parte; c. a bordo di un aeromobile immatricolato presso quella Parte; d. da un proprio cittadino, se l'infrazione è penalmente punibile nel luogo ove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato. Ogni Parte può riservarsi il diritto di non applicare o di applicare solo in condizioni o casi specifici le regole di competenza definite ai paragrafi 1.b - 1.d dell'articolo o in una parte qualunque di essi.

La Convenzione, però, all'art. 22, par. 4 esplicitamente non esclude alcuna competenza penale esercitata da una Parte in base al proprio diritto interno. Infine, al par. 5, caldeggia anche l'avvio di un proficuo dialogo tra Stati, qualora più di una Parte rivendichi la propria competenza per una presunta infrazione prevista dalla presente Convenzione al fine di stabilire la competenza più appropriata per esercitare l'azione penale.

Sul punto è intervenuta anche l'Unione europea, avendo essa notato il possibile nocumento che le rilevanti lacune e le notevoli differenze nel diritto e nelle procedure penali possono causare alla lotta alla criminalità organizzata e il terrorismo, nonché alla cooperazione giudiziaria in materia penale sviluppatasi o in corso di sviluppo in tale settore.

L'art. 12 della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio dispone che gli Stati membri stabiliscano la propria competenza giurisdizionale relativamente ai reati di cui agli articoli da 3 a 8 quando il reato sia stato commesso:

- a) in tutto o in parte sul loro territorio; o
- b) da un loro cittadino, quanto meno nei casi in cui l'atto costituisce un reato nel luogo in cui è stato commesso.

Nello stabilire la propria giurisdizione conformemente al paragrafo 1, lettera a), uno Stato membro assicura di avere competenza giurisdizionale qualora:

- a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; o
- b) il reato sia stato commesso contro un sistema di informazione nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato.

Uno Stato membro informa la Commissione ove decida di stabilire la competenza giurisdizionale per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora:

- a) l'autore del reato risieda abitualmente nel suo territorio; o
- b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio.

L'art. 12 della direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, in conformità alla direttiva 2013/40/UE, dispone che ciascuno Stato membro adotti le misure necessarie a stabilire la propria giurisdizione per i reati di cui agli articoli da 3 a 8 ove si verifichi uno o più dei casi seguenti:

- a) il reato è commesso, anche solo in parte, sul suo territorio;
- b) l'autore del reato è un suo cittadino.

Ai fini del paragrafo 1, lettera a), si ritiene che un reato sia stato commesso in tutto o in parte sul territorio di uno Stato membro quando l'autore commette il reato mentre era

fisicamente presente in quel territorio e, indipendentemente dal fatto che il sistema di informazione con cui è stato commesso il reato si trovasse o meno nel suo territorio.

Uno Stato membro informa la Commissione ove decida di stabilire la giurisdizione per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora:

- a) l'autore del reato risieda abitualmente nel suo territorio;
- b) il reato sia commesso a vantaggio di una persona giuridica che ha sede nel suo territorio;
- c) il reato sia stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio.

La direttiva 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio dispone all'art. 17 che: «Gli Stati membri adottano le misure necessarie a stabilire la propria giurisdizione per i reati di cui agli articoli da 3 a 7 nei seguenti casi:

- a) il reato è stato commesso in tutto o in parte sul loro territorio; oppure
- b) l'autore del reato è un loro cittadino.

2. Lo Stato membro informa la Commissione in merito alla decisione di stabilire la propria giurisdizione anche per i reati di cui agli articoli da 3 a 7 commessi al di fuori del suo territorio, tra l'altro nei casi seguenti:

- a) il reato è stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio;
- b) il reato è stato commesso a vantaggio di una persona giuridica che ha sede nel suo territorio; oppure
- c) l'autore del reato risiede abitualmente nel suo territorio.

3. Gli Stati membri provvedono affinché rientrino nella loro giurisdizione i casi in cui un reato contemplato dagli articoli 5 e 6 e, nella misura in cui sia pertinente, dagli articoli 3 e 7, sia stato commesso a mezzo di tecnologie dell'informazione e della comunicazione a cui l'autore ha avuto accesso dal loro territorio, a prescindere dal fatto che la tecnologia in questione sia basata o meno su tale territorio.

4. Per le azioni penali relative ai reati di cui all'articolo 3, paragrafi 4, 5 e 6, all'articolo 4, paragrafi 2, 3, 5, 6 e 7 e all'articolo 5, paragrafo 6, commessi al di fuori del territorio dello Stato membro interessato, per quanto riguarda il paragrafo 1, lettera b), del presente articolo, ciascuno Stato membro adotta le misure necessarie affinché la sua giurisdizione non sia subordinata alla condizione che i fatti costituiscano reato nel luogo in cui sono stati commessi».

Infine, l'art. 9 della decisione-quadro 2008/913/GAI sulla lotta contro talune forme ed espressioni di razzismo e xenofobia mediante il diritto penale, in relazione alla giurisdizione, dopo aver indicato i tradizionali principi della territorialità, della personalità attiva e del vantaggio per la persona giuridica, al comma 2 dispone che: «Nello stabilire la propria competenza giurisdizionale ai sensi del paragrafo 1, lettera a), ciascuno Stato membro adotta le misure necessarie per garantire che essa si estenda ai casi in cui il comportamento è posto in essere mediante un sistema di informazione e:

- a) l'autore pone in essere il comportamento allorché è fisicamente presente sul suo territorio, a prescindere dal fatto che il comportamento implichi o no l'uso di materiale ospitato su un sistema di informazione situato sul suo territorio;
- b) il comportamento implica l'uso di materiale ospitato su un sistema di informazione situato sul suo territorio, a prescindere dal fatto che l'autore ponga in essere o no il comportamento allorché è fisicamente presente sul suo territorio».

Stabilisce poi che uno Stato membro può decidere di non applicare o di applicare solo in casi o circostanze specifici la regola sulla competenza giurisdizionale di cui al paragrafo 1, lettere b) e c).

Sin qui, si può rilevare che da una parte la Convenzione sulla criminalità informatica adotta il criterio della territorialità¹⁷⁵ oppure, laddove il reato sia punibile nel luogo in cui è stato commesso ovvero non rientri nella competenza territoriale di nessuno Stato, il principio della personalità attiva¹⁷⁶; dall'altra le fonti dell'Unione europea indicano alternativamente i criteri della territorialità, della personalità attiva e, relativamente alle persone giuridiche, del destinatario del profitto¹⁷⁷.

Il criterio della territorialità appare entrato in crisi, poiché indebolito in tutti i casi in cui degli elementi di carattere informatico si innestano nella vicenda concreta o su aspetti processualistici. Si consideri, ad esempio, l'acquisizione di elementi di prova informatici, sempre più spesso collocati in rete e soggetti alla disciplina di altri Paesi o alla difficoltà di individuare il *locus commissi delicti* in ragione di un indirizzo IP che "balza" da uno Stato all'altro, al fine di eludere le attività investigative. In questi casi, il fenomeno a cui si assiste è spesso quello di una scissione tra *locus commissi delicti* e luogo di formazione della prova¹⁷⁸.

In Italia si assiste ad una commistione di principi. La disciplina italiana per alcuni aspetti si ispira al criterio di territorialità, per altri, invece, sembra aprirsi ad una vocazione espansiva. Infatti, vi è una combinazione dei diversi principi, senza che nessuno predomini in modo assoluto¹⁷⁹. Tuttavia, la dottrina dominante parla di principio di territorialità temperato¹⁸⁰.

Sul piano sostanziale, secondo l'art. 3, comma 1, c.p. i soggetti vincolati alla legge penale italiana sono i cittadini e gli stranieri che si trovino sul territorio dello Stato. Si tratta di una evidente affermazione del principio di territorialità, strettamente connesso con il concetto di sovranità e di indipendenza statale. Tuttavia, sono stabilite alcune eccezioni indicate dal diritto pubblico interno e dal diritto internazionale, in deroga al criterio della territorialità. Infatti, ai sensi del comma 2 la legge penale italiana obbliga

¹⁷⁵ Il criterio di territorialità fu teorizzato nel periodo in cui sorsero gli Stati indipendenti, tra il XVI ed il XVII secolo, e si lega all'impostazione nazionalistica della repressione dei reati. Secondo tale principio, la legge di uno Stato è vincolante per chiunque si trovi sul territorio, prescindendo dalla nazionalità dell'autore del reato, sul presupposto che il *locus commissi delicti* rappresenta il luogo di maggior allarme sociale, il posto dove è più agevole svolgere le indagini, e di conseguenza, il posto dove deve affermarsi la giustizia e ristabilire l'ordine sociale violato.

¹⁷⁶ In forza del principio della personalità attiva, ad ogni autore del reato viene applicata la legge dello Stato al quale appartiene. Ad esso si conforma il diritto internazionale, secondo il brocardo *leges ossibus inhaerent*, alla luce del nesso che intercorrerebbe tra l'individuo e il proprio diritto nazionale. In tal caso, lo Stato avrebbe sempre la giurisdizione sui propri cittadini, a prescindere dal luogo in cui essi si trovino e dal *locus commissi delicti*, perché *rei publicae interest habere bonos subditos*.

¹⁷⁷ Sul punto, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 150 ss.

¹⁷⁸ Al riguardo, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 154 ss.

¹⁷⁹ In tal senso, G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, Bologna, 2019, p. 143 ss.; T. TREVES, *La giurisdizione nel diritto penale internazionale*, Padova, 1973, p. 59.

¹⁸⁰ Il principio base è il principio di territorialità, ma sono stati apportati notevoli temperamenti attraverso l'adozione parziale di altri principi. Cfr., F. ANTOLISEI, *Manuale di diritto penale*, Milano, 2003, p. 108; G. BETTIOL, L. PETTOELLO MANTOVANI, *Diritto penale*, Padova, 1986, p. 174; F. MANTOVANI, *Diritto penale. Parte generale*, Milano, 2017, p. 881 ss; A. PAGLIARO, voce *Legge penale nello spazio*, in *Enc. giur.*, XXIII, Milano, 1973, p. 1054 ss.

anche tutti i cittadini o stranieri che si trovano all'estero, limitatamente ai casi stabiliti dalla legge o dal diritto internazionale¹⁸¹.

Secondo l'art. 6 c.p., si ritiene che il reato sia commesso nel territorio dello Stato quando l'azione o l'omissione è avvenuta in tutto o in parte su di esso, ovvero ivi si è verificato l'evento quale conseguenza dell'azione od omissione.

L'affermazione del principio di territorialità, temperato dagli altri criteri (personalità, difesa ed universalità), ha determinato, complice un rafforzamento della cooperazione giudiziaria internazionale, un progressivo superamento nell'uso del criterio di territorialità, alla luce dell'emersione di beni giuridicamente protetti di carattere non strettamente nazionale¹⁸².

Il legislatore per determinare il *locus commissi delicti* ha adottato il criterio dell'ubiquità. Secondo l'interpretazione maggioritaria, il reato si considera commesso nel territorio italiano quando al suo interno sia stato eseguito anche uno solo degli atti del processo criminoso necessari per la configurazione della fattispecie¹⁸³.

Orbene, la corretta determinazione del *locus commissi delicti* risulta fondamentale per individuare il giudice competente per territorio. La regola – come già chiarito – trova la propria *ratio* nell'esigenza di assicurare un effettivo controllo sociale, di rendere più agevole e rapida la raccolta della prova, ridurre i disagi per le parti e per i testi, ed infine di riaffermare il diritto e la giustizia nel luogo in cui sono stati violati, al fine di ristabilire l'ordine¹⁸⁴.

Ed invero, sul punto l'art. 8 c.p.p. indica, quale regola generale per determinare la competenza per territorio del giudice, il luogo in cui il reato è stato consumato. Nei commi successivi sono poi indicate altre regole di carattere generale che tuttavia derogano al criterio del *locus commissi delicti* in ragione della particolare configurazione della fattispecie criminosa. Nello specifico, se dal fatto ne è derivata la morte di una o più persone, è competente il giudice del luogo in cui è avvenuta l'azione o l'omissione; se si tratta di reato permanente, è competente il giudice del luogo in cui ha avuto inizio la consumazione, anche se dal fatto ne deriva la morte di una o più persone; in caso di delitto tentato, è competente il giudice del luogo in cui è stato compiuto l'ultimo atto diretto a commettere il delitto.

¹⁸¹ La nozione di cittadino e di territorio è contenuta nell'art. 4 c.p., mentre il riferimento al diritto internazionale evoca un mero inquadramento terminologico. Invero, lo straniero può essere processato penalmente solo se sussiste un collegamento con lo Stato del giudice. Per il diritto consuetudinario lo Stato può, ma non deve punire; può, ma non deve concedere l'estradizione dell'individuo allo Stato che intenda punirlo. Per quanto riguarda il diritto pattizio, numerose convenzioni contengono la regola *aut dedere aut iudicare* (o estradare o giudicare). Per un approfondimento, T. TREVES, *La giurisdizione nel diritto penale internazionale*, cit., p. 3 ss.

¹⁸² Sul punto, D. PULITANO, G. DODARO, sub *Art. 3 c.p.*, in AA.VV., *Commentario breve al codice penale* (a cura di G. FORTI, S. SEMINARA, G. ZUCALÀ), VI ed., Milano, 2017, p. 25 ss.; G. FIANDACA, G. LEINERI, sub *Art. 6 c.p.*, *ivi*, p. 36 ss.; M. RONCO, *La legge penale. Fonti, tempo, spazio, persone*, Bologna, 2016.

¹⁸³ Sul punto, L. PICOTTI, *La legge penale*, in AA.VV., *Giurisprudenza sistematica di diritto penale, codice penale, parte generale* (a cura di F. BRICOLA, F. ZAGREBELSKY), Torino, 1996, II, p. 17 ss.; G. FIANDACA, G. LEINERI, sub *Art. 6 c.p.*, cit., p. 36 ss.

¹⁸⁴ Così, in dottrina, A.A. DALIA, M. FERRAIOLI, *Manuale di diritto processuale penale*, cit., p. 92 ss.; F. DELLA CASA, G.P. VOENA, *Soggetti*, in AA.VV., *Compendio di procedura penale* (a cura di G. CONSO, V. GREVI, M. BARGIS), Milano, 2014, p. 17 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 75 ss. In giurisprudenza, Cass., SS.UU., 16 luglio 2009, n. 40537, in *Cass. pen.*, 2010, p. 2121.

Oltre queste, sono poi previste dall'art. 9 c.p.p. regole suppletive¹⁸⁵, le quali consentono di individuare il giudice competente territorialmente quando non è possibile applicare le regole di cui all'art. 8 c.p.p. Si tratta di regole suppletive e non alternative a quelle individuate all'art. 8 c.p.p., applicabili, dunque, solo quando risulta assolutamente impossibile individuare il giudice competente per territorio secondo le regole generali.

Queste regole vanno applicate nel rispetto della gerarchia interna alla norma. Ciò significa che va seguito l'ordine individuato dallo stesso legislatore e che è stato trasfuso all'interno dell'articolo. In tal modo, il legislatore ha scongiurato il rischio di una possibile lesione dell'art. 25, comma 1, Cost. secondo cui «nessuno può essere distolto dal giudice naturale precostituito per legge».

L'importanza del principio costituzionale si coglie sia nella posizione strategica in cui è stata collocata dai Padri costituenti, sia dagli importanti riflessi che si hanno nel campo dell'ordinamento giudiziario, essendo di conseguenza esclusa, mediante la previsione di un divieto assoluto, la possibilità di istituire giudici straordinari, ossia giudici *post factum*, su di cui, inoltre, sorgerebbero dubbi circa la propria parvenza di imparzialità e terzietà. Ciò risulta del tutto evidente se la norma è letta in combinato disposto con l'art. 102, comma 2, Cost.

La perfetta collocazione dell'art. 25 Cost. consente di ritenere che il principio sia stato formulato innanzitutto in funzione di garanzia dei cittadini. Ed invero, l'articolo è inserito nel Titolo I della Parte I della Costituzione, dedicata ai diritti e ai doveri dei cittadini, nell'ambito dei rapporti civili. Ciò consente di ritenere la scelta del legislatore del codice repubblicano pienamente soddisfacente del principio individuato. Infatti, la previsione di regole suppletive rappresenterebbe una proiezione del principio di legalità ed un perfetto bilanciamento tra le varie istanze costituzionalmente previste.

Ed invero, il sistema previsto dagli artt. 8 e 9 c.p.p. disegnerebbe un buon equilibrio tra il pieno rispetto del principio del giudice naturale precostituito per legge e l'esigenza di individuare comunque un giudice territorialmente competente, qualora le regole generali non siano applicabili, al fine di conseguire una rapida ed efficiente amministrazione della giustizia. A dimostrazione di ciò milita la posizione assunta nella sistematica gerarchica dal criterio del giudice competente in base al luogo in cui ha sede l'ufficio del pubblico ministero che per primo ha provveduto all'iscrizione della notizia di reato nel registro di cui all'art. 335 c.p.p.

Infatti, tale criterio è posizionato al comma 3, e quindi in posizione totalmente recessiva e subalterna a tutte le altre regole, ad indicare che l'applicazione di essa debba essere *extrema ratio*, in quanto quella meno garantista dei criteri costituzionali. Ciò perché una posizione di preminenza di essa potrebbe prestare il fianco ad ipotesi di *forum shopping*, per cui sarebbe l'ufficio inquirente/requirente a scegliere il giudice che dovrà poi decidere.

La dottrina ha osservato che «la difficoltà di individuare il *locus commissi delicti* negli illeciti realizzati con il mezzo informatico ha consegnato una eccessiva discrezionalità al pubblico ministero circa la scelta della sede giudiziaria ove incardinare inizialmente il

¹⁸⁵ Ai sensi dell'art. 9 c.p.p. «1. Se la competenza non può essere determinata a norma dell'articolo 8, è competente il giudice dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione.

2. Se non è noto il luogo indicato nel comma 1, la competenza appartiene successivamente al giudice della residenza, della dimora o del domicilio dell'imputato.

3. Se nemmeno in tale modo è possibile determinare la competenza, questa appartiene al giudice del luogo in cui ha sede l'ufficio del pubblico ministero che ha provveduto per primo a iscrivere la notizia di reato nel registro previsto dall'articolo 335».

procedimento»¹⁸⁶. Ciò ha dato luogo al fenomeno delle «superprocure che si autoinvestono del potere di acquisire notizie di reato e di indagare a tutto campo pur in assenza di qualsivoglia legittimazione territoriale»¹⁸⁷.

Man mano che ci si allontana dalle regole generali di cui all'art. 8 c.p.p. e ci si avvicina alla regola di cui all'art. 9, comma 3, c.p.p. si assisterebbe ad un affievolimento della garanzia di cui all'art. 25 Cost., ma comunque non al suo totale annichilimento, inserita pur sempre nel rispettoso contesto delle previsioni di cui all'art. 6 CEDU e all'art. 47 della Carta dei diritti fondamentali dell'Unione europea.

La questione, in relazione ai reati commessi e/o consumati nel *cyberspace* non è di poco conto. Come ricavabile dalla normativa richiamata, le fonti europee ed internazionali evitano di prendere posizione in ordine ai problemi profilabili in tema di giurisdizione e di competenza. Per cui, sul tema si è cominciato a dibattere in dottrina e la giurisprudenza ha provato a caldeggiare alcune soluzioni, in assenza di una disciplina specifica.

Nel caso della consumazione di un reato informatico, dunque, non è sempre possibile o agevole individuare il *locus commissi delicti*¹⁸⁸. Ciò porta a stabilire spesso la competenza mediante le regole di cui all'art. 9 c.p.p.¹⁸⁹, che – in quanto suppletive, sussidiarie e non alternative a quelle dell'art. 8 c.p.p. – non devono in alcun modo diventare preminenti rispetto alle regole generali. Un'ampia applicazione di queste regole comporterebbe la dilatazione della competenza ben al di là del dato territoriale, rischiando, tra l'altro, di espandere la giurisdizione italiana, ma provocando anche una incertezza del diritto del tutto inaccettabile in uno Stato di diritto basato sull'aureo principio di legalità in senso formale e sostanziale.

Eppure, in concreto, per tali tipologie di reato, le regole dell'art. 9 c.p.p., ed in particolare del comma 3, diventerebbero generali e non più sussidiarie, prestando il fianco ad una possibile e concreta lesione del principio costituzionale del giudice naturale precostituito per legge.

Ed invero, parte della dottrina ha osservato che «l'adozione del criterio di stretta sussidiarietà incide direttamente sulla legalità del processo, ove si consideri che se fosse ammissibile, da parte del titolare dell'azione penale o del giudice che deve decidere sul rinvio a giudizio, privilegiare a seconda dei casi l'uno o l'altro elemento, si verrebbe a riconoscere a codeste autorità un potere di scelta discrezionale del giudice, perfettamente

¹⁸⁶ Così testualmente, L. LUPÀRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in AA.VV., *Investigazione penale e tecnologia informatica* (a cura di L. LUPÀRIA, G. ZICCARDI) Milano, 2007, p. 155. Per un ulteriore approfondimento, E.M. CATALANO, *L'abuso del processo*, Milano, 2004, p. 155 ss.

¹⁸⁷ In questi termini, E. AMODIO, *Il processo penale tra disgregazione e recupero del sistema*, in *Verso la riscoperta di un modello processuale. Convegno in memoria di Antonino Galati*, Atti del Convegno. Caserta, 12-14 ottobre 2001, Milano, 2003, p. 35.

¹⁸⁸ Su tale annoso profilo, già K. CORNILS, *Il luogo di commissione dei reati di manifestazione del pensiero in internet*, in *Diritto dell'informazione e dell'informatica*, 4/5, 2002, p. 891 ss.; D. D'AGOSTINI, L. VIOLINO, *Le indagini nei reati informatici*, in AA.VV., *Diritto penale dell'informatica: dai computer crimes alla digital forensic* (a cura di D. D'AGOSTINI), Forlì, 2007, p. 175; D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004, p. 21 ss.; L. PICOTTI, *Profili penali delle comunicazioni illecite via internet*, in *Il Diritto dell'informazione e dell'informatica*, 2, 1999, 320 ss.; S. SEMINARA, *La pirateria su internet e il diritto penale*, in *AIDA. Annali italiani del diritto d'autore, della cultura e dello spettacolo*, 5, 1996, p. 183 ss.

¹⁸⁹ In tal senso, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 156.

analogo a quello che in passato fu riconosciuto in contrasto con il principio del giudice naturale»¹⁹⁰.

Ulteriore problematica involge la qualità di reati istantanei, ovvero di durata, dei *cybercrime*. Aspetto di maggior attenzione dovrebbe essere la propalazione degli effetti nello spazio: è lo stesso fatto tipico che, «nella parte in cui si realizza *tramite* i sistemi informatici, si deve ritenere che si protragga, espanda ed eventualmente “riproduca” in quei suoi elementi essenziali» dipendenti dall’esecuzione delle funzioni automatizzate, «pur non sempre del tutto “dominabili” dai titolari, gestori e fruitori dei sistemi stessi»¹⁹¹.

Infine, il tema investe totalmente le problematiche relative alle regole applicabili per la formazione della prova. Le incertezze, inoltre, coinvolgono in pieno anche l’ampia costellazione degli istituti volti a regolare i rapporti con le autorità straniere. Invero, in caso di mandato di arresto europeo avente ad oggetto una richiesta di consegna delle Autorità rumene per il reato di accesso abusivo ad un sistema informatico o telematico, la Cassazione ha stabilito che «il divieto di consegna previsto dall’art. 18, comma primo, lett. p), della legge n. 69 del 2005, presuppone che la giurisdizione italiana in ordine al “*locus commissi delicti*” risulti con certezza, non potendosi ritenere sufficiente la mera ipotesi che il reato sia stato commesso in tutto od in parte nel territorio dello Stato»¹⁹². La Suprema Corte ha dunque escluso la giurisdizione italiana, non essendo stato accertato il luogo in cui si trovava la postazione utilizzata dall’agente per superare le misure di sicurezza apprestate dal *server* della società, a nulla rilevando che il predetto *server* fosse collocato in territorio italiano.

Le *questiones* proposte sinora potrebbero essere affrontate con un approccio casistico. Il metodo empirico consentirebbe di rendere maggiormente evidenti le problematiche sinora esposte in ordine sparso, sino a condurre ad una – si spera – felice sintesi che possa indicare un compromesso o una soluzione *de iure condendo*.

Per alcuni reati, quale ad esempio la diffamazione consumatasi via *web*, è stato affermato che «rispetto all’offesa della reputazione altrui realizzata via Internet, ai fini dell’individuazione della competenza, sono inutilizzabili, in quanto di difficilissima, se non impossibile individuazione, criteri oggettivi unici, quali, ad esempio, quelli di prima pubblicazione, di immissione della notizia in rete, di accesso del primo visitatore. [...] Non è neppure utilizzabile quello del luogo in cui è situato il *server* (che può trovarsi in qualsiasi parte del mondo), in cui il *provider* alloca la notizia». Pertanto, la conclusione a cui arriva la Cassazione è che «la competenza per territorio per il reato di diffamazione, commesso mediante la diffusione di notizie lesive dell’altrui reputazione allocate in un sito della rete “Internet”, va determinata in forza del criterio del luogo di domicilio dell’imputato, in applicazione della regola suppletiva stabilita dall’art. 9, comma secondo, cod. proc. pen.»¹⁹³.

Con tale arresto, la giurisprudenza si è arresa all’evidenza, ossia all’impossibilità di applicare i criteri di cui all’art. 8 c.p.p., individuando di fatto nell’art. 9 c.p.p. i criteri da

¹⁹⁰ In tali termini, U. NANNUCCI, *Le regole di competenza quali norme strumentali al principio del giudice naturale*, in *Dir. pen. e proc.*, 4, 1995, p. 461 ss.

¹⁹¹ Così, L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d’insieme*, cit., p. 35 ss.; ID., *Reati informatici, riservatezza e identità digitale*, report presentato al VII Convegno Nazionale dei Professori di Diritto Penale sul tema “Il diritto penale tra recenti modifiche e progetti di riforma”, Torino, 9-10 novembre 2018. V., anche, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 154.

¹⁹² Cass., Sez. VI, sentenza del 30 giugno 2015, n. 27825, in *CED Cass.*, rv. 264055 – 01.

¹⁹³ Cfr., Cass., Sez. I, sentenza del 15 marzo 2011, n. 16307, in *CED Cass.*, rv. 249974 – 01; conf., Cass., Sez. I, sentenza del 21 dicembre 2010, n. 2739, in *CED Cass.*, rv. 249179 – 01.

applicare in tali ipotesi. Infatti, ove risulti impossibile individuare il luogo di consumazione del reato, ma sia invece determinabile quello in cui il contenuto diffamatorio è stato caricato come dato informatico, la competenza territoriale va determinata ai sensi dell'art. 9, comma 1, c.p.p., in relazione al luogo in cui è avvenuta una parte dell'azione. Ma, a ben vedere, anche questo criterio risulta praticamente inapplicabile, per cui dovrà farsi ricorso al criterio di cui all'art. 9, comma 2, c.p.p. secondo cui il giudice territorialmente competente sarà quello della residenza, dimora o domicilio dell'imputato¹⁹⁴.

Altre diverse conclusioni ermeneutiche si rintracciano in caso di truffa realizzata mediante l'utilizzo di strumenti tecnologici o della rete. Si pensi alle ipotesi di acquisto di beni *online* mai ricevuti compiuti mediante ricariche su prodotti bancari denominati "Postepay", non abbinati a conti correnti.

Un primo orientamento, coerente sul piano sostanziale, ritiene che il *locus commissi delicti* sia ravvisabile nel luogo di destinazione del pagamento, ovvero nel luogo in cui avviene l'incasso o è accettata la disposizione patrimoniale. Ciò perché, tradizionalmente, il reato di truffa si consuma con l'effettivo conseguimento del bene economico o di altro bene che sia idoneo ad una valutazione patrimoniale, con la definitiva perdita di esso da parte del soggetto passivo¹⁹⁵. Senonché, così ritenendo, il luogo nel quale il profitto viene conseguito coinciderebbe con quello nel quale viene successivamente utilizzata la carta, ossia tendenzialmente con qualsiasi posto in cui sia posizionato uno sportello ATM sul territorio statale o anche col domicilio dell'indagato, dal momento che tali strumenti di pagamento sono utilizzati soprattutto *online*¹⁹⁶. Si potrebbe configurare, allora, una ipotesi di *forum shopping*.

La conclusione logica sarebbe, dunque, ancora una volta quella di optare per una generale disapplicazione dei criteri di cui all'art. 8 c.p.p. a vantaggio dei criteri residuali contemplati all'art. 9 c.p.p., i quali diverrebbero di fatto criteri generali per i reati consumati con tali modalità. In particolare, sia la dottrina che la giurisprudenza osservano che in tal caso sarebbe individuabile quale competente solo il giudice del luogo di residenza, dimora o domicilio dell'imputato¹⁹⁷.

Senonché, la Cassazione è intervenuta stabilendo che «nel delitto di truffa, quando il profitto è conseguito mediante accredito su carta di pagamento ricaricabile (nella specie postepay), il tempo e il luogo di consumazione del reato sono quelli in cui la persona offesa ha proceduto al versamento del denaro sulla carta, poiché tale operazione ha realizzato contestualmente sia l'effettivo conseguimento del profitto da parte dell'agente,

¹⁹⁴ Sul punto, Cass., Sez. V, sentenza del 19 maggio 2015, n. 31677, in *CED Cass.*, rv. 264521 – 01, secondo cui «Nei reati di diffamazione tramite la rete "internet", ove sia impossibile stabilire il luogo di consumazione del reato e sia stato invece individuato quello in cui il contenuto diffamatorio è stato caricato come dato informatico, per poi essere immesso in rete, la competenza territoriale va determinata, ai sensi dell'art. 9, primo comma, cod. proc. pen., in relazione al luogo predetto, in cui è avvenuta una parte dell'azione».

¹⁹⁵ Cass., SS.UU., sentenza del 22 marzo 1969, n. 2, in *CED Cass.*, rv. 111418 – 01.

¹⁹⁶ Sul punto, C. PECORELLA, *Truffe online: momento consumativo e competenza territoriale*, in *penalecontemporaneo.it*, 10 febbraio 2012.

¹⁹⁷ In tal senso, C. PECORELLA, *Truffe online: momento consumativo e competenza territoriale*, cit.; in giurisprudenza, Tribunale di Aosta, sentenza del 29 settembre 2011, n. 579/11, in cui si afferma il principio in base al quale nell'ipotesi di truffa *online* realizzata mediante piattaforma elettronica con pagamento avvenuto mediante ricarica *Postepay*, «poiché è ignoto il luogo nel quale l'imputato avrebbe effettivamente avuto la disponibilità della somma accreditatagli sulla predetta carta, la competenza territoriale deve essere individuata, in base ai criteri suppletivi di cui all'art. 9, comma 2, c.p.p., nel luogo di residenza dell'imputato».

che ottiene l'immediata disponibilità della somma versata, e non un mero diritto di credito, sia la definitiva diminuzione patrimoniale in danno della vittima¹⁹⁸», ristabilendo così l'operatività del criterio dettato dall'art. 8, comma 1, c.p.p., seppur in modo "creativo".

Questa regola, per quanto consta l'orientamento della Procura Generale presso la Corte di cassazione, non sarebbe applicabile in caso di bonifico bancario. In tale ipotesi, sarebbe attribuito nuovamente un rilievo decisivo al luogo nel quale è stata resa disponibile la somma di denaro, per effetto del positivo esito del disposto bonifico bancario¹⁹⁹. Ciò però si scontrerebbe con l'impossibilità di individuare secondo tale criterio il giudice competente per territorio in tutti i casi – sempre più frequenti – in cui gli istituti bancari operino solo in rete e siano privi di sportelli o sezioni territoriali, ovvero non facilmente individuabili in relazione a pagamenti attraverso bonifico bancario²⁰⁰. In tali casi, ancora una volta verrebbe fatta ampia applicazione dei criteri di cui all'art. 9 c.p.p., con l'estremo pericolo di lesione dei principi costituzionalmente garantiti.

Si assiste, dunque, alla tendenza a «“bypassare” la regola generale di cui all'art. 8 c.p.p. [...] a causa della difficoltà, rispetto a condotte o parti di condotte che si realizzano nello spazio cibernetico, a delimitare tale luogo e, spesso, ad accertare la “provenienza” dell'autore del fatto, ovvero la tracciabilità delle operazioni poste in essere tramite l'indispensabile “mediazione” degli strumenti informatici e telematici»²⁰¹.

Ma probabilmente le fattispecie di maggior interesse possono essere quelle relative a reati informatici o cibernetici in senso stretto. L'analisi delle complesse questioni sinora affrontate diventa particolarmente intrigante per l'interprete quando si imbatte nello studio della giurisprudenza in tema di competenza del giudice in ipotesi di accesso abusivo a sistemi informatici o telematici²⁰².

¹⁹⁸ Cass., Sez. II, sentenza del 6 ottobre 2017, n. 3329, in *Guida al diritto*, 17, 2018, p. 83.

¹⁹⁹ Cfr. PROCURA GENERALE DELLA REPUBBLICA PRESSO LA CORTE SUPREMA DI CASSAZIONE, *Decr. N. 65/09 R.D. del 17.03.2009*; nello stesso senso, ID., *Decr. N. 228/10 R.D. del 05.07.2010*; in precedenza, ID., *Decr. N. 28/08 R.D. del 24.01.2008*.

²⁰⁰ Così, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 167.

²⁰¹ Così, testualmente, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 160.

²⁰² Ci si riferisce all'art. 615-ter c.p., il quale recita: «Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio».

Per quanto attiene alla competenza per territorio del giudice, si sono sviluppati due orientamenti tra loro contrari²⁰³. Secondo il primo, competente per territorio è il giudice del luogo in cui l'autore del reato si è connesso alla rete effettuando il collegamento logico con il sistema; il secondo orientamento²⁰⁴ sostiene che il giudice competente territorialmente sia quello del luogo ove è collocata la banca dati costituente oggetto di intrusione.

Nel tentativo di risolvere il contrasto giurisprudenziale, le Sezioni unite della Corte di cassazione²⁰⁵ hanno aderito alla tesi che individua il luogo della consumazione del reato in quello in cui si trova il soggetto che effettua l'introduzione abusiva o si mantiene nello spazio informatico senza l'autorizzazione del titolare²⁰⁶.

La soluzione adottata trova il proprio fondamento nella presa d'atto dello stato di alterazione nella realtà virtuale rispetto all'impostazione tradizionale del concetto di azione penalmente rilevante, dovuto alla smaterializzazione ed alla delocalizzazione di risorse e contenuti trasfusi nel *web*. L'orientamento della Corte risulta poi rafforzato dalla consapevolezza della complessità aterritoriale della rete, consolidata ulteriormente dalla diffusione di *devices* e dal *cloud computing*²⁰⁷.

Pertanto, la Corte non ha potuto far altro che stabilire che il luogo ove si radica la competenza del giudice è quello dove avviene l'accesso, il quale «inizia con l'unica condotta umana di natura materiale, consistente nella digitazione da remoto delle credenziali di autenticazione da parte dell'utente, mentre tutti gli eventi successivi assumono i connotati di comportamenti comunicativi tra il client e il server».

Infatti, la Suprema Corte ha affermato che «se l'azione dell'uomo si è realizzata in un certo luogo – sia pur attraverso l'uso di uno strumento informatico e, dunque, per sua natura destinato a produrre flussi di dati privi di una loro “consistenza territoriale” – non v'è ragione alcuna per ritenere che quel “fatto”, qualificato dalla legge come reato, non si sia verificato proprio in quel luogo, così da consentire la individuazione di un giudice anche “naturalisticamente” (oltre che formalmente) competente».

²⁰³ Sulla differenza tra proposizioni opposte e proposizioni contrarie, F. CORDERO, *Procedura penale*, cit., p. 375, secondo cui «[d]a Ermagora a Quintiliano, la teoria degli “*status causae*” descrive figure dialettiche a battute opposte o contrarie [...]. Date due proposizioni, le definiamo opposte quando abbiano lo stesso tema e una sia preceduta dal segno “non” (o “è falso che...”); una deve essere vera, anzi lo è, perché p e non-p esauriscono l'universo logico; impossibile che siano tutt'e due false [...] (tertium non datur). Sono contrarie quando, se una fosse vera, l'altra sarebbe falsa, ma niente esclude che siano entrambe false [...]».

²⁰⁴ Cass., Sez. I, sentenza del 27 maggio 2013, n. 40303, in *Riv. it. dir. e proc. pen.*, 3, 2014, p. 1502 ss., con commento di C.F. GROSSO, *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, p. 1518; nonché in *Cass. pen.*, 5, 2014, p. 1704 ss., con nota di S. ATERNO, *OSSERVAZIONI a Cass. Pen., 27 maggio 2013, n. 40303, sez. I*, p. 1706.

²⁰⁵ Cfr., Cass., SS.UU., sentenza del 26 marzo 2015, n. 17325, con commento e rilievi critici di R. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, cit., p. 1296 ss.

²⁰⁶ Sul punto, M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *penalecontemporaneo.it*, 2 febbraio 2015; P. DE MARTINO, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico*, in *penalecontemporaneo.it*, 11 maggio 2015.

²⁰⁷ In tal senso, R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 177 ss.

Tale posizione è stata criticata dalla dottrina²⁰⁸, la quale ha fatto notare come in tali contesti l'attività umana «spesso trova come tramite infiniti processi di automazione e non si riduce al mero inserimento di credenziali di autenticazione in un sistema informatico attraverso la digitazione su una tastiera». Ad esempio, l'autore del reato potrebbe utilizzare un *device* di sua proprietà o solo in suo possesso per accedere ad Internet attraverso diversi *servers*, *Internet Service Providers* e sistemi delocalizzati rispetto al luogo in cui materialmente si trova.

In tali contesti è difficile localizzare e tracciare l'esatto luogo in cui si è avuto l'accesso abusivo. Inoltre, spesso con l'indirizzo IP è possibile individuare solo il Paese in cui è avvenuto l'accesso, e non anche il luogo geografico esatto. Sovente, a causa anche delle tecniche di distorsione dell'indirizzo IP, che consentono il “salto del segnale”, non è neanche individuabile con certezza il Paese da dove è partito l'impulso logico generato dall'attività umana finalizzato all'accesso abusivo. Ulteriori difficoltà si ravvedono quando si opera in contesti quali il *cloud*.

Infine, l'orientamento della Corte di Cassazione potrebbe incentivare il *forum shopping*: un autore del reato potrebbe preferire luoghi fisici per l'accesso abusivo ove la magistratura adotta indirizzi giurisprudenziali più favorevoli. Anzi, alla luce delle riforme in discussione, tali reati potrebbero essere difficilmente perseguiti se non inseriti nei criteri di priorità di cui dovranno dotarsi le Procure della Repubblica, una volta ultimato il *restyling* del procedimento penale.

In un simile contesto, va totalmente rivisto l'approccio in materia di giudice competente per territorio. È necessario, infatti, squarciare il “velo di Maya” che occulta alla vista degli operatori quella che è la realtà di queste nuove fattispecie, tutte caratterizzate dalla smaterializzazione, atterritorialità e delocalizzazione.

Un nuovo approccio, moderno e al passo con i tempi, deve necessariamente tenere in debita considerazione il nuovo contesto tecnologico in cui si sviluppano tali reati, ricorrendo ad un approccio culturale parzialmente scollato dall'ambito tradizionale.

Di particolare interesse risulta l'orientamento adottato di recente dalla Corte di cassazione in tema di adescamento di minorenni, fattispecie astratta tipizzata all'art. 609-*undecies* c.p.²⁰⁹, secondo cui «il reato di adescamento di minorenni, previsto dall'art. 609-*undecies* cod. pen., si consuma nel tempo e nel luogo in cui l'agente realizza le condotte descritte nella fattispecie incriminatrice; tuttavia, qualora l'illecito sia posto in essere tramite internet o con mezzi di comunicazione a distanza, la sua consumazione si verifica nel luogo in cui si trova il minore adescato, perché il delitto presuppone una comunicazione tra due soggetti e in tale luogo si perfeziona la dimensione offensiva del fatto»²¹⁰.

Tale orientamento ha il pregio di aver indicato un approccio legato al luogo in cui vi è l'effettiva lesione del bene giuridicamente protetto, ossia il luogo in cui si trova il minore adescato o, in maniera più specifica, dell'area informatica di pertinenza del

²⁰⁸ R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 183 ss.

²⁰⁹ L'art. 609-*undecies* c.p. recita: «Chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-*bis*, 600-*ter* e 600-*quater*, anche se relativi al materiale pornografico di cui all'articolo 600-*quater*.1, 600-*quinquies*, 609-*bis*, 609-*quater*, 609-*quinquies* e 609-*octies*, adesci un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione».

²¹⁰ Cass., Sez. III, sentenza del 26 giugno 2019, n. 36492, Rel. A. Di Stasi, in *CED Cass.*, rv. 276684-01.

titolare a prescindere dal luogo in cui si trova il terminale dell'agente o da quello in cui si trova il server.

Questo orientamento lega la questione del *locus commissi delicti* alla titolarità del bene giuridico protetto, con riferimento, dunque, non solo alla esecuzione della condotta esteriore richiesta per la sussistenza del reato da parte dell'autore, ma, soprattutto, al momento di partecipazione al delitto da parte della persona offesa e, quindi, alla concretizzazione dell'offesa del bene-interesse tutelato.

Per individuare il giudice competente per territorio, dunque, bisognerebbe sganciarsi dalla logica tradizionale di ambiente territoriale, per abbracciare una visione che tenga conto di un nuovo spazio: lo spazio virtuale, nel quale gli utenti, i programmi, i dati e i sistemi sono connessi tra di loro e possono migrare ed interagire. Seguendo questo percorso, una buona soluzione potrebbe essere l'analisi del luogo fisico in cui l'offensività raggiunge la sua dimensione maggiore.

Una simile impostazione, che sembra ripercorrere in parte il recente arresto giurisprudenziale, rischierebbe però di dare adito ad una giurisprudenza "creativa" o ad interpretazioni che tendono ad appiattirsi sui criteri sussidiari dettati dall'art. 9 c.p.p. Ciò tenderebbe a ricreare un circolo vizioso che l'interprete del processo penale deve in tutti i modi evitare: rendere anche solo uno dei criteri sussidiari un criterio generale per alcuni tipi di reato, con conseguente lesione del principio del giudice naturale precostituito per legge.

Allora, una soluzione *de iure condendo* rispettosa dello Stato di diritto e del principio di legalità in senso formale e sostanziale potrebbe essere quella di creare per queste tipologie di reato una nuova regola generale che si aggiunge a quelle già contemplate all'art. 8 c.p.p. che individui il giudice competente per territorio in base all'area informatica – *rectius*, lo spazio informatico – di pertinenza del titolare del bene giuridicamente protetto, con particolare riferimento al luogo in cui si manifestano gli effetti dell'offesa.

Tale regola non sembra creare problematiche applicative di qualunque tipo, poiché nel caso in cui lo spazio informatico coincida con un luogo fisico, ivi si cristallizzerebbe la competenza per territorio. Si pensi all'accesso abusivo ad un sistema informatico alle banche dati del Comune di Roma. In tale ipotesi, la competenza sarebbe del Tribunale di Roma. Diversamente, se lo spazio informatico di pertinenza del titolare non sia fisicamente o territorialmente individuabile, la regola consentirebbe di individuare comunque un luogo fisico ove radicare la competenza del giudice in ragione del rapporto che si instaura tra persona offesa, bene giuridicamente protetto e spazio informatico.

Il principio troverebbe conforto anche nella giurisprudenza dell'Unione europea. Invero, la Corte di giustizia ha affermato che «la vittima di una lesione di un diritto della personalità per mezzo di Internet può adire un foro, a seconda del luogo di concretizzazione del danno cagionato da detta lesione nell'Unione europea, per la totalità di tale danno. Poiché l'impatto, sui diritti della personalità di un soggetto, di un'informazione messa in rete può essere valutata meglio dal giudice del luogo in cui la presunta vittima possiede il proprio centro di interessi, l'attribuzione di competenza a tale giudice corrisponde all'obiettivo di una buona amministrazione della giustizia»²¹¹, nonché al principio di economia processuale.

²¹¹ Sul punto v., Corte di giustizia, Grande Sezione, sentenza del 25 ottobre 2011, *eDate Advertising GmbH e a. contro X e Société MGN LIMITED*, cause riunite C-509/09 e C-161/10, ECLI:EU:C:2011:685, punto 48. V. anche, Corte di giustizia, Sez. I, sentenza del 19 aprile 2012, *Wintersteiger AG contro Products 4U Sondermaschinenbau GmbH*, causa C-523/10, ECLI:EU:C:2012:220, punto 18.

In assenza di una simile regola generale, il principio formulato potrebbe trovare applicazione mediante un ragionamento logico-sistematico che rappresenta comunque il frutto di una creatività ragionata finalizzata ad una soluzione ermeneutica evolutiva.

Infatti, la dottrina non ha mancato di osservare che il principio del legame persona offesa, spazio informatico e bene giuridico protetto potrebbe comportare l'applicazione di uno dei criteri individuati dall'art. 9 c.p.p. Ed invero, il giudice competente dovrebbe essere quello del luogo in cui è avvenuta una parte dell'azione, ai sensi dell'art. 9, comma 1, c.p.p., ossia quello in cui si trova l'area informatica violata che, se non è territorialmente definibile, dovrà essere individuata mediante il nesso con il suo titolare²¹².

Purtroppo, come già osservato, una simile impostazione sconta dei dubbi circa il rispetto del principio del giudice naturale precostituito per legge e del principio di legalità sostanziale²¹³, in quanto essenzialmente farebbe assurgere a criterio generale una regola suppletiva, da applicare solo quando nel caso concreto non è possibile individuare la competenza del giudice mediante una delle regole di cui all'art. 8 c.p.p. La regola suppletiva, allora, rischierebbe di diventare, per tali tipi di reato, regola generale, con conseguente lesione dei principi costituzionali sottesi a garanzia del processo.

Più semplicemente, la previsione di una regola generale potrebbe condurre all'individuazione del giudice competente in base alla sede ovvero alla residenza, domicilio o dimora del titolare del bene giuridico protetto, in quanto è lì che questi possiede il proprio centro di interessi²¹⁴.

²¹² Cfr., R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, cit., p. 190.

²¹³ Per principio di legalità formale si intende la necessità di una base legale per ogni atto dell'amministrazione. Tale accezione è propria delle democrazie parlamentari. Il principio troverebbe attuazione con la mera predisposizione di norme attributive del potere, senza che siano necessarie norme vincolanti. Sul punto, L. CARLASSARE, *Regolamenti dell'esecutivo e principio di legalità*, Padova, 1966. Seguendo tale prospettiva, si conclude che gli atti, per essere legali, non devono essere contrari o incompatibili con le norme processuali. Per principio di legalità sostanziale, invece, si intende la corrispondenza dell'atto non solo al modello legale di riferimento, ma anche alle indicazioni dell'ordinamento costituzionale. Infatti, si potrebbe sostenere che la legalità in senso formale si riferirebbe al profilo della conformità degli atti al rispettivo modello legale previsto dal legislatore, mentre la legalità sostanziale riguarderebbe la correttezza del procedimento, intesa come equità, ossia come effettivo rispetto dei principi costituzionali posti a tutela della persona, fulcro dell'intero procedimento, e che in virtù dell'art. 2 della Costituzione si pone al centro di tutto l'ordinamento giuridico. Sul punto anche, C. IASEVOLI, *La nullità nel sistema processuale penale*, Napoli, 2008, p. 58 ss.

²¹⁴ Cfr., Corte di giustizia, Grande Sezione, sentenza del 25 ottobre 2011, *eDate Advertising GmbH e a. contro X e Société MGN LIMITED*, cause riunite C-509/09 e C-161/10, ECLI:EU:C:2011:685, secondo cui, poiché l'impatto sui diritti della personalità di un soggetto di un contenuto messo in rete può essere valutato meglio dal giudice del luogo in cui la presunta vittima possiede il proprio centro di interessi, l'attribuzione di competenza a tale giudice corrisponde all'obiettivo di una buona amministrazione della giustizia. Tale luogo, in linea generale, corrisponde alla residenza abituale della vittima, ma può trattarsi anche di uno Stato membro in cui la vittima non risiede abitualmente, ove altri indizi, quali l'esercizio di un'attività professionale, possano dimostrare l'esistenza di un collegamento particolarmente stretto con tale Stato.

La competenza del giudice del luogo in cui la vittima ha il proprio centro di interessi è conforme all'obiettivo della prevedibilità delle norme sulla competenza anche nei confronti del convenuto, poiché chi emette l'informazione lesiva, al momento dell'immissione in rete della stessa, è in condizione di conoscere i centri d'interessi delle persone che ne formano oggetto. Il criterio del centro d'interessi consente, al contempo, all'attore di individuare agevolmente il giudice al quale può rivolgersi e al convenuto di prevedere ragionevolmente dinanzi a quale giudice può essere citato.

5. Il “dedalo” nozionistico della prova digitale e le sue caratteristiche

Il *cyberspace* non va assolutizzato. Non è solo bene o solo male, ma consente opportunità e progresso pur in un contesto che può dar luogo a degenerazioni socialmente riprovevoli e da perseguire penalmente. Si potrebbe ritenere che il bene ed il male siano due valori assoluti. In realtà il confine tra loro è *quite permeable*, è del tutto permeabile²¹⁵. Il mondo dell'informatica e delle nuove tecnologie consente, *inter alia*, di formare prove relative a reati – anche comuni²¹⁶ – connotati da circostanze che coinvolgono strumenti tecnologici. In ciò si manifesta un'essenza positiva²¹⁷.

Scrivere di prova informatica crea particolare disagio e profonda inquietudine. Di fatto, l'impatto delle nuove tecnologie e, in particolare, della prova informatica nel processo penale si colora di una relativa contrapposizione tra opposti i cui confini sono permeabili e sfumati. L'evoluzione tecnologica – in quanto elemento di questo mondo e frutto dell'uomo – manifesta una sorta di ambivalenza, il cui nucleo è composto da elementi positivi ed elementi negativi. Essere consapevoli di ciò non giustifica il “male” che essa contiene, ma la “democratizza”, la rende maggiormente sondabile.

L'ambivalenza dello sviluppo tecnologico si manifesta nella fruibilità di esso sia da parte della criminalità, la quale la sfrutta per commettere reati, sia da parte dello Stato per la prevenzione e repressione dei reati.

Si parla di indagine informatica sia quando questa è diretta all'identificazione dell'autore di crimini informatici, sia se si utilizzano tecnologie informatiche e telematiche nello svolgimento delle investigazioni sui reati comuni²¹⁸.

²¹⁵ Secondo Zimbardo è possibile sviluppare una prospettiva morale e politica diversa, che tralasci qualunque logica binaria e tendenza essenzialistica. «Il male consiste nel comportarsi intenzionalmente in modi che danneggiano, oltraggiano, umiliano, deumanizzano o distruggono altre persone innocenti – o nell'usare la propria autorità e il proprio potere sistemico per spingere altri, o consentire ad altri, di farlo per noi». In tale contesto, in quanto persone, anche i colpevoli non devono essere danneggiati, oltraggiati, umiliati, deumanizzati o distrutti. Il male è «sapere ciò che è meglio ma fare il peggio». Cfr. P. ZIMBARDO, *L'effetto Lucifero. Cattivi si diventa?*, Milano, 2008, p. 1 ss.

²¹⁶ Per la dottrina è pacifico che «le indagini informatiche appaiono oggi in progressiva espansione lungo ogni settore dell'investigazione penale, a partire dal procedimento che vedono coinvolti i cosiddetti *computer crimes* in senso lato» descritti dagli studiosi anglosassoni con l'immagine “*old wine in new bottles*”. Le statistiche confermano che la frequenza della commissione di tali reati è cresciuta esponenzialmente con l'avvento dei *cybercrime* commessi in rete. In questi termini, L. LUPÀRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, cit., p. 131. In tal senso anche L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet* (a cura di L. PICOTTI), cit., p. 26; F. RESTA, *Virtualità del crimine. Dai reati informatici ai cybercrimes*, in *L'informatica nel diritto*, Supplemento a “Giurisprudenza di merito”, 2006, p. 102. Si veda, altresì, S.B. HOAR, *Trend in cybercrime: the dark side of the internet*, in *Criminal Justice*, 3, 2005, p. 4.

²¹⁷ Sui vantaggi e i rischi delle nuove tecnologie, C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, 3, 2019, p. 1167 ss.

²¹⁸ Così, P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Diritto penale e processo*, 4, 2011, p. 493. Sulla rilevanza dell'elemento di prova digitale per l'accertamento di qualsiasi tipo fatto-reato, F. BUFFA, *Internet e criminalità. Finanza telematica off shore*, Milano, 2011; D. CACCAVELLA, *Informatica forense e linea del tempo*, Relazione presentata al convegno “Nuove prospettive sui reati informatici”, Venezia, 27 maggio 2006, paper; E. CASEY, *Digital evidence and computer crime. Forensic science, computers and the internet*, London-San Diego, 2000, p. 199; V. MILITELLO, *Informatica e criminalità organizzata*, in *Riv. trim. dir. pen. econ.*, 1990, p. 81.

Mentre la società tende sempre più a svilupparsi sulla base delle nuove tecnologie e l'uso di dispositivi mobili aumenta, un numero crescente di apparecchiature tecnologiche è utilizzato dal crimine e quindi molto spesso sequestrato dalle forze dell'ordine come fonte di prova. Questi dispositivi sono impiegati dai criminali per comunicare, archiviare dati e facilitare i crimini. Computer, telefoni cellulari, dispositivi GPS, fotocamere digitali e altri sistemi che contengono prove digitali devono essere adeguatamente raccolti, gestiti ed elaborati. Altri elementi sono poi individuabili in internet.

Oggi, quasi ogni azione umana rischia di lasciare una traccia digitale. Lo *smartphone* sta assumendo sempre più le forme di una nuova estensione del corpo²¹⁹. Inoltre, diventa di fondamentale importanza per la vita quotidiana l'utilizzo di alcuni strumenti tecnologici in grado di generare una traccia digitale.

Dai social network, allo *smartwatch*, passando per le automobili. Qualsiasi apparecchio elettronico oggi è in grado di generare un elemento digitale utilizzabile in futuro come potenziale prova in un processo penale a favore o contro le persone coinvolte. La rapida evoluzione tecnico scientifica offre al processo penale nuovi strumenti utili alla ricostruzione del fatto, ampliando notevolmente i settori ove le nuove tecnologie e l'apporto scientifico possono apportare un contributo fondamentale²²⁰.

Le prove digitali non sono informazioni che possono essere utilizzate in un processo penale solo nel caso di un reato che si connota unicamente di aspetti informatici. Spesso sono utili anche per i reati comuni, tant'è che oggi risulta arduo immaginare reati che non abbiano in qualche modo una dimensione "digitale"²²¹.

Preliminarmente, va chiarito che l'analisi scientifica dell'attuale disciplina va letta sistematicamente, tenendo conto di una duplice prospettiva: il rispetto dell'ampia gamma di diritti difensivi e delle libertà della persona e quella connessa all'esigenza di attendibilità dell'accertamento²²².

Non esiste una definizione univoca ed universalmente riconosciuta di prova informatica o prova digitale. In letteratura scientifica sembrano essere accettate e comunemente utilizzate uniformemente entrambe le terminologie, senza proporre una sostanziale differenza semantica.

Le legislazioni nazionali spesso non includono riferimenti diretti ed espliciti alle fonti di prova digitale e prova informatica, né tantomeno propongono una loro definizione specifica ed esclusiva. Ciò perché è davvero complesso dare un inquadramento concettuale alle prove digitali²²³.

²¹⁹ In tema, S. RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Milano, 2009, p.81, secondo il quale è possibile parlare di «corpo elettronico», perché «pezzi» di persone sono conservati nelle numerosissime banche dati dove le identità personali sono sezionate e scomposte. Il corpo assume una nuova conformazione ed è definito come una unità funzionale, comprendente anche entità fisicamente collocate in luoghi diversi.

²²⁰ In tal senso, P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p.1377 ss. Sulle possibili lesioni ai diritti fondamentali da parte della tecnologia, G. DI PAOLO, «Tecnologie del controllo» e prova penale, Padova, 2008; S. MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalia*, 2006, p. 387 ss.

²²¹ Cfr., M.A. BIASIOTTI, S. CONTI, F. TURCHI, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1640.

²²² Sul punto, L. LUPÀRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 141 ss.

²²³ «Sul punto occorre intendersi fin da subito. Ben può utilizzarsi la formula *digital evidence*, o prova digitale, quale recipiente ove includere ogni forma di utilizzo a fini procedimentali, in senso lato, di dati

Innanzitutto, bisogna distinguere il sistema informatico dai dati, laddove il sistema informatico consente l'archiviazione o l'elaborazione di questi, mentre i dati, i programmi e le informazioni assumono una propria individualità costituendo documenti informatici.

Si è affermato che la nozione di dato informatico, sebbene riferibile ai dati, programmi ed informazioni e, più in generale, alla componente *software* di un sistema, «risulta comunque non chiaramente definita se non per l'ampia indicazione dell'oggetto fisico, il quale, tuttavia, può assumere conformazioni diverse, potendo, ad esempio, riguardare un insieme di istruzioni formulate in uno specifico linguaggio e finalizzate alla esecuzione di determinate operazioni (come nel caso del programma applicativo), un mero insieme di informazioni come quelle conservabili su carta, il risultato dell'elaborazione di più informazioni o operazioni, la rappresentazione di atti, fatti, o dati giuridicamente rilevanti (nella forma, quindi, del documento elettronico), la riproduzione per immagine di atti o documenti cartacei etc».

Tuttavia, quando si discute di dato informatico, è alla definizione contenuta all'art. 1, lett. d) della Convenzione di Budapest a cui far generico riferimento, secondo il quale per dato informatico deve intendersi «qualunque rappresentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione».

Il termine *digital evidence* è stato coniato negli Stati Uniti d'America. In particolare, l'utilizzo del termine *evidence* implica, nel mondo anglosassone, la destinazione giudiziale del dato digitale, il quale viene raccolto per finalità indiziarie o probatorie all'interno di un processo²²⁴.

Lo standard ISO/IEC 27037:2012, *Guidelines for identification, collection, acquisition, and preservation of digital evidence* intende per prove digitali i dati già in formato digitale, ma non inserisce in tale categoria quelli convertiti da analogici in digitali. Mentre lo *Scientific Working Group on Digital Evidence* – che tra le altre cose ha stilato numerose *best practices* per il trattamento delle prove digitali – ritiene prova digitale «ogni informazione di valore probativo trasmessa o conservata in formato digitale»²²⁵.

La dottrina definisce la prova digitale come «il complesso delle informazioni digitali che sono in grado di stabilire se un crimine è stato commesso o che possono rappresentare un collegamento tra un crimine e le sue vittime o i suoi esecutori»²²⁶. Recentemente, lo stesso autore, riprendendo la definizione del Chisum, è ritornato sulla definizione: «le prove digitali sono informazioni conservate o trasmesse attraverso un computer che rifiutino o supportino una teoria su come un fatto sia accaduto o che forniscono elementi

originariamente contenuti in supporti informatici o telematici, oppure ancora trasmessi in modalità digitale. A patto, però, di tenere a mente che si tratta di un fenomeno con diverse sfaccettature, che mal si presta a inquadramenti a priori ed è difficilmente conciliabile con le tradizionali distinzioni in tema di prova. Più in particolare, la natura multiforme del dato digitale sconsiglia generalizzazioni aprioristiche». M. PITTIRUTI, *Digital evidence e procedimento penale*, Torino, 2017, p. 8.

²²⁴ In tal senso, P. PERRI, voce *Computer forensics (indagini informatiche)*, in *Dig. disc. pen.*, cit., p. 100 ss.

²²⁵ SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE), INTERNATIONAL ORGANIZATION ON DIGITAL EVIDENCE (IOCE), *Digital Evidence: Standards and Principles*, in *Forensic Science Communications*, 2, 2000, p. 2. I documenti sono consultabili su www.swgde.org.

²²⁶ In tali termini, E. CASEY, *Digital Evidence and Computer Crime. Forensic science, computers and the Internet*, London-San Diego, 2000, p. 196 ss.

risolutivi quali l'alibi o il movente»²²⁷. Ma anche questa ultima definizione, nel citare come sistema informatico solo il computer, non sembra convincente, poiché limitativa ed obsoleta, alla presenza della vasta gamma di dispositivi oggi capaci di raccogliere, elaborare e trasmettere i dati²²⁸, a differenza, invece, della definizione data dal Consiglio d'Europa, più precisa su questo specifico punto.

Pertanto, è stato proposto di definire la prova elettronica come «un dato (compresi quelli generati da dispositivi analogici o digitali) che è manipolato, conservato o comunicato da un dispositivo controllato da una persona, da un computer o trasmesso con il supporto di un sistema di comunicazione, che ha la capacità di avere valore probativo e dimostrare una tesi in modo più efficace di come una parte potrebbe fare senza il suo ausilio»²²⁹.

Secondo una definizione più tecnica fornita dall'*International Organization of Computer Evidence* (IOCE), la *digital evidence* consiste in qualsiasi informazione trasmessa o memorizzata in formato binario suscettibile di essere utilizzata in sede processuale²³⁰. Questa definizione è stata criticata dalla dottrina perché si concentra eccessivamente sul valore processuale del dato informatico. Inoltre, il riferimento al codice binario ridurrebbe eccessivamente a solo alcune possibili modalità di manifestazione dei dati digitali²³¹.

La dottrina italiana non si è concentrata solo sull'essenza di essa, ma ha ampliato la panoramica, facendo attenzione anche alla sua consistenza empirica. Secondo tale orientamento «si può considerare *digital evidence* ogni informazione probatoria la cui rilevanza processuale dipende dal contenuto del dato o dalla particolare allocazione su di una determinata periferica, oppure dal fatto di essere stato trasmesso secondo modalità informatiche o telematiche»²³².

Altra parte della dottrina ritiene che per prove digitali debbano intendersi «quelle fonti di prova memorizzate in qualsiasi tipo di strumento informatico come ad esempio gli *smartphone*, palmari, telefoni cellulari, server aziendali, postazioni di lavoro dei dipendenti, o altri sistemi cosiddetti informatici o telematici complessi (es. Cloud Computing)»²³³.

²²⁷ Così, E. CASEY, *Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet*, Amsterdam, 2011, p. 840.

²²⁸ In tal senso, B. SCHAFER, S. MASON, *The Characteristics of Digital Evidence*, in S. MASON, *Electronic Evidence*, London, 2012, p. 25.

²²⁹ In questi termini, B. SCHAFER, S. MASON, *The Characteristics of Digital Evidence*, cit., p. 25. Gli autori spiegano che questa definizione è basata su tre elementi: 1) comprende tutte le forme di prove; 2) include le varie forme di dispositivi con cui i dati possono essere conservati o trasmessi; 3) sottolinea l'aspetto della rilevanza (essendo l'ammissibilità un criterio che il giudice valuta sulla base di diversi principi) e pertanto «restrict the definition of electronic evidence to those items offered by the parties as part of the fact-finding process».

²³⁰ Cfr., *amplius*, L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007, p. 60.

²³¹ Così, E. CASEY, *Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet*, cit., p. 840.

²³² L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 12, 2011, p. 4509B. Per un approfondimento sulla tecnologia informatica nell'investigazione penale, L. LUPARIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007.

²³³ Con queste parole, S. ATERNO, voce *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen.*, cit., p. 217 ss.

Nell'ambito del progetto “*Evidence*”, il gruppo di lavoro ha proposto la seguente definizione: «*Electronic Evidence is any information of potential or tangible probative value that is generated through, stored on or transmitted by any electronic device*»²³⁴.

Una definizione generalmente accettata è stata elaborata dal Consiglio d'Europa. Secondo la “Guida alla prova digitale” per fonti di prova digitale si intendono le «informazioni generate, memorizzate o trasmesse mediante dispositivi elettronici che possono essere utilizzate in giudizio»²³⁵. Inoltre, si raccomanda di preservare l'integrità delle informazioni acquisite e scambiate nonché di garantire la tracciabilità di ogni passaggio svolto.

La proposta di Regolamento relativa agli ordini europei di produzione e di conservazione definiscono le prove elettroniche come «le prove conservate in formato elettronico dal prestatore di servizi o per suo conto al momento della ricezione del certificato di ordine europeo di produzione o di conservazione, consistenti nei dati conservati relativi agli abbonati, agli accessi, alle operazioni o al contenuto»²³⁶.

La giurisprudenza italiana ha dato risalto all'aspetto investigativo, in particolar modo concentrandosi sui dati soggettivistici che potrebbero ricavarsi dall'informazione digitale. La *digital evidence* è stata, dunque, definita come «il risultato di attività d'indagine volta sia all'identificazione dell'autore di crimini informatici, sia all'identificazione, mediante l'impiego di procedure informatiche, dell'autore di reati comuni, anche se non commessi col mezzo informatico»²³⁷.

Sembra, però, che per ottenere una definizione completa ed onnicomprensiva sia necessario unire gli elementi specifici di ogni definizione sinora data. Per prova elettronica si può ritenere quell'informazione generata, memorizzata, trasmessa o convertita in formato digitale mediante dispositivi elettronici, allocata in una determinata periferica od in un *cloud*²³⁸ e legalmente formata nel procedimento penale, dalla quale possono ricavarsi fatti o circostanze che si riferiscono all'imputazione, alla punibilità e alla determinazione della pena o della misura di sicurezza, utili per l'accertamento della verità processuale.

Tale nozione non può trascurare quanto indicato dallo *Scientific Work Group on Digital Evidence* (SWGDE), secondo cui l'acquisizione di una informazione digitale avrà inizio proprio quando le informazioni e/o l'hardware verranno raccolti o immagazzinati a scopo d'esame per la formazione della prova in un processo²³⁹; né tantomeno trascura la natura prismatica e multiforme della *digital evidence*. Infatti, «la natura informatica del dato da cui trarre il risultato probatorio può vertere sia direttamente sul *thema probandum*

²³⁴ Per questa definizione, S. AVVEDUTO, D. LUZI, L. PISACANE, *La categorizzazione del progetto Evidence: la rappresentazione concettuale del dominio “prova elettronica*, in *Informatica e diritto*, 1-2, 2015, p. 189.

²³⁵ Cfr., CONSIGLIO D'EUROPA, *Guida alla prova digitale*, Strasburgo, 2013, p. 13, disponibile al sito www.coe.int/cybercrime.

²³⁶ Cfr., Art. 2 della proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, COM (2018) 225 final, 2018/0108(COD).

²³⁷ Cfr., Cass., Sez. I, sentenza del 6 novembre 2018, n. 50021.

²³⁸ La dottrina ha evidenziato che la fonte di prova digitale può riguardare sia un ambiente “statico” come un computer, sia un ambiente “dinamico”, come ad esempio la rete. Cfr., G. ZICCARDI, *Aspetti informatico-giuridici della fonte di prova digitale*, in AA.VV., *Investigazione penale e tecnologia informatica* (a cura di L. LUPÀRIA, G. ZICCARDI), cit., p. 49.

²³⁹ Si veda il paper SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE), INTERNATIONAL ORGANIZATION ON DIGITAL EVIDENCE (IOCE), *Digital Evidence: Standards and Principles*, in *Forensics Science Communications*, April 2000, II, n. 2, consultabile all'URL <http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm>.

sia su un fatto secondario da cui poter risalire al fatto principale: quale esempio del primo tipo v'è l'immagine pedopornografica in formato digitale il cui possesso è contestato all'imputato; quale esempio del secondo tipo possono addursi i file di log circa l'avvenuto accesso ad un social network per mezzo di un computer localizzato sulla *scena criminis* ove è stato commesso un omicidio nella medesima finestra temporale»²⁴⁰.

Poiché le procedure giuridiche in vigore nei diversi Paesi europei sono preesistenti alla comparsa della prova elettronica, in genere non esiste una normativa *ad hoc*. Gli Stati hanno, quindi, tentato in vario modo di colmare le lacune normative createsi, senza però prestare attenzione ad una necessaria armonizzazione, tenuto conto della natura transnazionale della prova digitale²⁴¹. Ancora oggi, manca un quadro comune europeo di riferimento per guidare i decisori politici, le forze dell'ordine e le autorità giudiziarie nel trattamento e nello scambio delle prove elettroniche, nonostante i tempi siano maturi per la creazione di uno strumento comune per la formazione di esse non solo tra Stati membri dell'Unione europea. L'Unione europea sta lavorando proprio a ciò.

Peculiarità della prova digitale sono: l'universalità, l'immaterialità, la dispersione, la promiscuità, la modificabilità, la volatilità, l'attitudine ad essere copiata all'infinito.

Per universalità si intende la vasta fruibilità della prova digitale nel processo penale per qualsiasi tipo di reato, non solo informatico, dovuto alla diffusione sempre maggiore dei sistemi informatici e della digitalizzazione delle conoscenze nella società moderna, nonché alle interconnessioni tra il mondo fisico e il mondo digitale²⁴².

L'immaterialità riflette l'evidente incorporeità della prova digitale. Essa conserva una propria fisicità, essendo un conglomerato di impulsi elettrici che rispondono ad una logica numerica prestabilita basata sul sistema binario e che sono convogliati in un sistema informatico²⁴³. Tuttavia, la fisicità di tale entità non è percepibile all'essere umano in assenza del supporto informatico in cui viene innestata²⁴⁴.

²⁴⁰ Così, M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., p. 8 ss.

²⁴¹ In tal senso, S. AVVEDUTO, D. LUZI, L. PISACANE, *La categorizzazione del progetto Evidence: la rappresentazione concettuale del dominio "prova elettronica"*, cit., p. 182.

²⁴² In questi termini, M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2, 2011, p. 283 ss.; C. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Milano, 2010, p. 7 s.

²⁴³ Pertanto, sulla base di tale considerazione, parte della dottrina ritiene che la terminologia possa sembrare non del tutto corretta, e considera che sarebbe più preciso far riferimento ai dati digitali utilizzando la nozione di "intangibilità". Tuttavia, è ormai consolidato l'utilizzo del termine immaterialità nel contesto giuridico con riferimento alla prova informatica, con accezione atecnica e come evocativo della mancanza di una corporeità tangibile. Così, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 122, spec. nota 1.

²⁴⁴ Cfr., M. DANIELE, *La prova digitale nel processo penale*, cit., p. 283 ss.; S. ATERNO, *Acquisizione e analisi della prova informatica*, cit., p. 61. Sull'immaterialità anche, S. ATERNO, voce *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen.*, cit., p. 217 ss.; L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4509B ss.; F.M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2, 2012, p. 696 B ss.; R. BORRUSO, S. RUSSO, C. TIBERI, *L'informatica per il giurista*, Milano, 2009, p. 118-119; A. GHIRARDINI, G. FAGGIOLI, *Computer forensics*, Milano, 2007, passim; A. MASUCCI, *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Riv. dir. civ.*, 1, 2004, p. 755 ss.; R. ORLANDI, *Questioni attuali in tema di processo ed informatica*, in *Riv. dir. processuale*, 1, 2009, p. 135; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 122; F. SIRACUSANO, *Prove informatiche*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX convegno nazionale. Roma, 20-21 ottobre 2016* (a cura di L. KALB), Milano, 2017, p. 250; P. TRONCONE, *La tutela penale del nuovo documento dematerializzato tra vicende novative e nuove aspirazioni sistematiche*, in *Riv. pen.*, 2008, p. 1277 ss. V., anche, R. FLOR, *La Corte di Giustizia considera la Direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2, 2014, p. 190, secondo il quale la rivoluzione informatica e

La potenziale dispersione della prova digitale è dovuta al fatto che le prove digitali di un reato sono allocate in *servers* e in *personal computers* fisicamente molto lontani. Infatti, la dispersione può riguardare l'intero pianeta Terra, tenuto conto dell'estensione mondiale delle reti informatiche²⁴⁵.

Corollario dell'immaterialità è la promiscuità del dato digitale ossia la collocazione di esso all'interno di uno spazio virtuale enorme e potenzialmente sconfinato, mescolato con un numero incredibilmente elevato di altri dati digitali²⁴⁶. La prova spesso è inclusa in contenitori dall'ampia capienza, talvolta fisicamente piccolissimi, ma in grado di accogliere un'elevatissima quantità di dati²⁴⁷. Essi, quindi, spesso sono invisibili ad un occhio inesperto: la fonte di prova digitale si trova spesso in luoghi dove solo gli specialisti la cercherebbero o è raggiungibile solo con strumenti molto specifici. Tale indagine, però, rischia di compromettere la riservatezza dell'utente, il quale potrebbe vedere pregiudicato il proprio diritto a causa di rivelazioni di informazioni riservate e sensibili relative alla sua persona o di segreti industriali attinenti all'ente coinvolto nel processo penale.

L'immaterialità comporta anche una congenita modificabilità della prova digitale. I dati contenuti in un sistema informatico sono facilmente alterabili da parte di chiunque ne disponga. I rischi che le prove digitali siano contraffatte o manipolate, volontariamente oppure a causa dell'impiego di tecniche di conservazione e salvataggio sbagliate, sono altissimi²⁴⁸. Nel processo penale, quindi, spesso si pongono questioni relative alla genuinità dell'elemento di prova digitale acquisito. Pertanto, è necessario garantire l'autenticità e la genuinità di esse attraverso il rispetto di *best practice* e di linee guida capaci di assicurare la protezione da alterazioni del dato informatico.

Le prove digitali possono essere danneggiate o distrutte anche per responsabilità degli stessi investigatori, consulenti o parti processuali non adeguatamente preparati, i quali

la velocità con cui si evolve hanno «trasformato i dati e le informazioni in “beni immateriali” di inestimabile valore».

²⁴⁵ Sul punto, *ex multis*, M.L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. internet*, 5, 2008, p. 503 s.

²⁴⁶ In tal senso, M. DANIELE, *La prova digitale nel processo penale*, cit., p. 283 ss. V., anche, T. LINARDI, *Sequestro probatorio – il sequestro probatorio e la “copia” dei dati informatici*, in *Giur. it.*, 10, 2019, p. 2286 ss.; F. SIRACUSANO, *Prove informatiche*, cit., p. 251.

²⁴⁷ Partendo dalla definizione di sistema informatico elaborata dalla Convenzione di Budapest, la Cassazione ha distinto il contenitore dal contenuto, ritenendo di dover valutare l'oggetto di un eventuale provvedimento di sequestro alla luce di ciò. Infatti, secondo l'orientamento prevalente, in base alla concreta necessità, sembrerebbe possibile sequestrare l'intero sistema – come, ad esempio, nel caso in cui l'apprensione sia necessaria per esaminare grosse quantità di dato, pur essendo necessaria la immediata restituzione decorso il tempo ragionevole utile per gli accertamenti in corso – ovvero il singolo dato, che ha certamente una sua identità fisica, essendo modificabile e misurabile. Cfr., Cass., SS.UU., sentenza del 7 settembre 2017, n. 40963. In tal senso, anche, Cass., Sez. VI, sentenza dell'11 novembre 2016, n. 53168, in *Ced Cass. rv. 268489*; Cass., Sez. VI, sentenza del 20 giugno 2015, n. 24617, in *Ced Cass. rv. 264093*. Pertanto, anche la componente *software* di un sistema informatico, avendo una sua consistenza compiutamente individuabile, può pacificamente ritenersi suscettibile di sequestro. Cfr., Cass., SS.UU., sentenza del 29 gennaio 2015, n. 31022, in *Ced Cass. rv. 264089*. In dottrina, L. BARTOLI, *Sequestro dei dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. Pen. online*, 1, 2018, p. 1 ss.; A. MARI, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati*, in *Cass. pen.*, 12, 2017, p. 4303 ss.; P. RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Cass. pen.*, 1, 2018, p. 131 ss.; G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in *Dir. pen. cont.*, 11, 2017, p. 157 ss.

²⁴⁸ Così, M. DANIELE, *La prova digitale nel processo penale*, cit., p. 283 ss.

maneggiano maldestramente il dato. Ciò può determinare problematiche relative alla genuinità della prova che poi si formerà in dibattimento²⁴⁹.

La tutela della genuinità della prova rappresenta un aspetto assolutamente centrale della tematica, strettamente collegata a quelli della cristallizzazione del “quadro” informatico attraverso complesse operazioni tecniche e della tracciabilità delle attività compiute sul medesimo attraverso la stesura di dettagliati *reports*, idonei a garantire il cosiddetto *chain of custody*, ossia la catena di custodia²⁵⁰.

Il dato informatico è poi anche altamente volatile²⁵¹, per cui oltre ai pericoli per la genuinità, si pongono anche esigenze relative alla dispersione probatoria. Invero, la fonte di prova digitale si trova a volte su dispositivi nei quali lo stato della memoria viene sovrascritto ogni volta che un determinato evento si verifica, con conseguente perdita dell’informazione elettronica. I dispositivi sui quali potrebbero trovarsi fonti di prova digitale devono essere posti in condizioni sicure il più rapidamente possibile.

Infine, le informazioni digitali possono essere copiate all’infinito e ogni copia sarà esattamente come l’originale. Questa proprietà unica consente la realizzazione di più copie esatte dell’originale idonee ad essere distribuite e analizzate allo stesso tempo da specialisti diversi. Permette anche che fonti di prove informatiche possano essere esibite esattamente come sono in tribunale contemporaneamente alla relazione del consulente tecnico²⁵².

Secondo rilevante dottrina, il tratto caratterizzante della prova digitale e, di conseguenza, del documento informatico non sta nella immaterialità. Infatti, non sarebbe questa la differenza rispetto al documento tradizionale. «La caratteristica ed anche la peculiarità del documento informatico è quella di essere veicolato su di uno strumento virtuale, il file, ed è questo ad essere incorporato [*eventualmente*, ndr.] su di una base materiale. Ecco perché il documento informatico deve essere definito come “dematerializzato”»²⁵³.

Dall’analisi delle definizioni proposte e delle caratteristiche possedute dalla prova digitale è possibile trarre alcune importanti conclusioni utili per questo lavoro. Innanzitutto, non esiste una netta differenza semantica tra prova digitale ed informatica, consentendo di ritenere entrambi sinonimi. Tuttavia, potrebbe affermarsi che mentre la

²⁴⁹ In questi termini, S. ATERNO, *Acquisizione e analisi della prova informatica*, cit., p. 62.

²⁵⁰ Così, L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4509B ss. Per un primo approccio alla *chain of custody*, L. LUPÀRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 147-149.

²⁵¹ Cfr., A. CHIARI, *La prova digitale: le sentenze sulla rilevanza probatoria e l’acquisizione*, in *Quot. Giur.*, 26 luglio 2018; F. SIRACUSANO, *Prove informatiche*, cit., p. 251.

²⁵² Cfr., CONSIGLIO D’EUROPA, *Guida alla prova digitale*, Strasburgo, 2013, p. 14, disponibile al sito www.coe.int/cybercrime.

²⁵³ Così, testualmente, P. TONINI, *L’evoluzione delle categorie tradizionali: il documento informatico*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1313. Per un approfondimento sul documento, v., *ex multis*, L. KALB, *Il documento nel sistema probatorio*, Torino, 2000, in particolare p. 71 ss. Secondo l’A. «l’idea di documento conduce subito la mente ad una cosa dotata della intrinseca capacità di trasmettere all’esterno quelle informazioni che sono in essa contenute. Il documento assolve così alla triplice funzione di rappresentare, di dimostrare e di informare in relazione al fatto cui si riferisce: si parla di funzione rappresentativa poiché grazie alla percezione del suo contenuto il documento è in grado di far conoscere ovvero di offrire alla mente la rappresentazione del fatto al quale si riferisce. A tale funzione sono connesse anche quella dimostrativa, intesa come funzione probatoria, e quella informativa, relativa al processo di formazione del documento stesso». Ed ancora, «con il termine documento, pertanto, si intende far riferimento a ciò che è diretto a rappresentare qualcosa: l’oggetto della rappresentazione è specificato nell’art. 234 in “fatti, persone o cose” ovvero tutto ciò che risulta rappresentabile attraverso mezzi idonei a fissarne la memoria storica».

prova digitale consiste in un dato digitale formatosi già con tali caratteristiche, la prova elettronica farebbe riferimento non solo ai dati inclusi nell'insieme "prova digitale", ma anche ai dati analogici convertiti successivamente in dati digitali, comprendendo tutte le prove che manifestino in qualche modo elementi di informatizzazione. In tal senso, la prova digitale sarebbe una *species* del *genus* prova elettronica.

Non esiste una definizione universalmente accettata di prova digitale se non quella proposta dal Consiglio d'Europa, che, però, non trova omologa conferma nell'ordinamento italiano attraverso una definizione che la ricalchi.

Le prove digitali *stricto sensu* sono elementi dotati di capacità dimostrativa «che esistono indipendentemente dall'inchiesta penale e rispetto ai quali le attività di ricerca, apprensione e analisi degli investigatori possono assumere una natura "statica" o "dinamica"»²⁵⁴.

Inoltre, le caratteristiche proprie della prova digitale evidenziano come questa sia essenzialmente un dato fragile: è necessario prestare particolare attenzione alle modalità di formazione e conservazione di essa poiché basterebbe anche solo un piccolo errore per rendere il dato inutilizzabile, disperdendo l'informazione.

Ed invero, la *digital evidence* non può essere ritenuta una "prova perfetta"²⁵⁵. Simile conclusione è una mera illusione perché essa non può dare – in ogni caso – alcuna garanzia di assoluta certezza nell'accertamento del fatto²⁵⁶. Se è vero che il trattamento dell'informazione digitale impone ai protagonisti del procedimento penale il rispetto di particolari e rafforzate cautele, nonché l'esatta osservanza delle regole dettate dal legislatore e dalla comunità scientifica per l'acquisizione del dato; non è altrettanto vero che l'elemento di prova scaturito dalla fonte sia materiale considerabile intrinsecamente genuino e pienamente rispettoso dei diritti fondamentali coinvolti²⁵⁷.

²⁵⁴ Le attività statiche hanno ad oggetto l'acquisizione di dati già conservati nella memoria del computer o del dispositivo elettronico, per cui si procede ad acquisizione *ex post*; si tratta invece di attività dinamica quando i dati vengono captati mentre circolano nel *cyberspace*, ossia mentre la trasmissione è in corso: in tal caso si parla di captazione in tempo reale. In entrambe le ipotesi si tratta di attività probatoria avente ad oggetto dati digitali di matrice extraprocedimentale. Per questa distinzione, F. SIRACUSANO, *Prove informatiche*, cit., p. 252.

²⁵⁵ Cfr. L. LUPÀRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, cit., p. 143 ss.

²⁵⁶ Sull'assenza di certezze assolute della prova scientifica, E. AMODIO, *Il diritto delle prove penali nel pensiero di Mirjan Damaška*, in *Riv. it. dir. e proc. pen.*, 1, 2007, p. 15.

²⁵⁷ Si pensi ad una conversazione avvenuta su *smartphone* mediante la piattaforma "Whatsapp". La conversazione può essere "catturata" con la tecnica dello "screenshot", successivamente stampata e presentata in processo quale elemento di prova. Tuttavia, nella successione degli eventi, nulla esclude che si sia inserito un fatto del tutto spiacevole: l'alterazione dell'informazione. Ed invero, utilizzando tali modalità non è possibile ritenere con certezza che, ad esempio, quella conversazione sia avvenuta proprio con il presunto autore del reato o che non siano stati cancellati alcuni messaggi nella singola conversazione sul telefono da cui si è provveduto a catturare l'immagine senza il rispetto delle garanzie e dei protocolli. Infatti, qualcuno potrebbe aver "portato in scena" una conversazione mai avvenuta con la persona individuata quale possibile autore del reato. È l'ipotesi in cui Tizio salvi nella rubrica del proprio *smartphone* un numero telefonico in proprio uso collegandolo però al profilo di un'altra persona. Nella chat di "Whatsapp" il nome del profilo sarà appunto quello dell'altra persona, ad esempio "Caio". Inoltre, Tizio potrebbe essere così scaltro da inserire anche una immagine profilo di Caio. A questo punto, potrebbe inscenare una conversazione, catturare l'immagine, stamparla e presentarla al processo. In tal caso, da questo indizio potrebbe solo "apparire" un fatto fenomenicamente avvenuto. L'elemento di prova dovrebbe essere ritenuto inattendibile perché assunto senza il rispetto delle forme e delle garanzie previste, posto che il codice di rito non ha stabilito alcuna sanzione processuale in caso di mancata loro adozione, necessitando, però, la valutazione, in concreto, della sussistenza di eventuali alterazioni dei dati originali e la corrispondenza ad essi di quelli estratti.

Per evitare ciò, sono state elaborate linee guida o *best practice*. L'ordinamento italiano, però, non indica né nel codice di procedura penale né in altre leggi le linee guida a cui far riferimento, né tantomeno sono sempre formalizzate dettagliatamente all'interno di protocolli nazionali o internazionali, comunque privi di valore giuridico e di vincolatività²⁵⁸. Conseguenza è che possono essere utilizzate linee guida diverse per la conservazione e formazione della prova informatica. Invero, la mancata "copertura" per le nuove tecnologie accertative propone periodicamente il problema delle regole processuali con le quali avvalersi di questi strumenti²⁵⁹.

Non va taciuta, del resto, la formidabile efficacia investigativa della prova digitale²⁶⁰, la quale, in ogni caso, non può spingere l'interprete ed il legislatore sino a ritenere la scienza – ed in particolar modo quella inerente all'informatica – una "regina delle prove"²⁶¹, dovendosi sempre ribadire con forza l'esclusione dal nostro ordinamento processual-penalistico di qualsiasi forma o vanto della prova legale²⁶².

Tuttavia, l'ampio ventaglio di linee guida o *best practice* attualmente esistenti comporta che alcune di esse possano non esser riconosciute come efficaci nei diversi ordinamenti, creando problemi per la circolazione della prova tra ordinamenti statuali. Ciò diventa ancor più importante se si tiene conto della naturale propensione della prova

Per un approfondimento sull'indirizzo giurisprudenziale relativo all'esclusione dell'inutilizzabilità in tali ipotesi, Cass., Sez. V, sentenza del 3 marzo 2017, n. 22695, in *CED Cass.*, rv. 270139; Cass., Sez. V, sentenza del 16 novembre 2015, n. 11905, in *CED Cass.*, rv. 266477.

²⁵⁸ Così, C. CONTI, *La prova informatica e il mancato rispetto della best practice: lineamenti sistematici sulle conseguenze processuali*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p.1330. Sui principi fondamentali che ispirano i protocolli, M. MATTIUCCI, *Le indagini sui reperti invisibili. High tech crime*, in AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze* (a cura di D. CURTOTTI, L. SARAVO), Torino, 2013, p. 715. Con riferimento alla prova digitale, si veda il *Best Practice Manual for the Forensics Examination of Digital Technology*, versione del 1.11.2015, adottato dall'ENFSI (*European Network of Forensic Science Institute*)

in http://enfsi.eu/wp-content/uploads/2016/09/1_forensic_examination_of_digital_technology_0.pdf. Nel manuale si fanno riferimenti generici alle modalità con le quali deve essere formata e trattata la prova digitale. L'ENFSI è stato fondato nel 1995 con lo scopo di rafforzare lo scambio di informazioni nel campo delle scienze forensi.

²⁵⁹ In tal senso, G. SPANGHER, *Le prove informatiche*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1304. Secondo l'A. «L'alternativa che si prospetta è quella tra il riferito ricorso alla prova atipica avverso l'estensione delle previsioni esistenti, quando non si evita di risolvere la questione, facendo riferimento ad un esito probatorio della responsabilità deducibile da altri elementi di prova».

²⁶⁰ Così, P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, cit., p. 1378. V., inoltre, G. RANALDI, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo - Rassegna Online*, 2, 2020, disponibile al link: <https://doi.org/10.6092/2421-0528/7031>.

²⁶¹ Per questa espressione, C. CONTI, *La prova informatica e il mancato rispetto della best practice: lineamenti sistematici sulle conseguenze processuali*, cit., p. 1331.

²⁶² Il processo penale si basa sul principio del libero convincimento del giudice. Questi è comunque tenuto a motivare le proprie ragioni in modo razionale secondo attendibilità degli elementi di prova e credibilità delle fonti, applicando di conseguenza le massime di esperienza e le leggi scientifiche necessarie al caso concreto, secondo logica ed in aderenza alle risultanze processuali. Questo principio non è accettato dagli Stati che adottano decisioni mediante l'istituto della giuria, la quale esprime un verdetto non motivato riassumibile nelle espressioni tra loro contrarie "colpevole" e "non colpevole". Da ciò ne deriva che il nostro ordinamento non può accettare l'istituto della prova legale nel processo penale. Ed invero, l'istituto della prova legale trova cittadinanza nel processo civile ogni qual volta sia il legislatore a sostituirsi al libero convincimento del giudice nella valutazione dell'elemento di prova, come avviene ad esempio nel caso della confessione. Di converso, nel processo penale, la confessione è sempre liberamente valutabile dal giudice, secondo i canoni di attendibilità e credibilità. *Eadem ratio* per la prova informatica. Per un'analisi sul punto, P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 245 ss.

informatica alla circolazione tra Stati o a formarsi in luoghi diversi dallo Stato in cui si consuma un reato e in cui si radicherà il processo.

Pertanto, è necessario sondare la natura transnazionale della prova informatica al fine di comprendere anche le finalità delle iniziative poste in campo dall'Unione europea relativamente alla formazione della prova tra Stati membri dell'Unione europea e con Stati terzi.

6. La natura intrinsecamente transnazionale della prova digitale. Piano dell'opera

La prova digitale ha una vocazione transfrontaliera che trascende la natura transnazionale del reato. Anche il reperimento di informazioni relative ad un reato inserito in un contesto strettamente nazionale potrebbe richiedere la ricerca e l'accesso a dati informatici conservati in un altro Stato o, addirittura, in un luogo non perfettamente sovrapponibile con il tradizionale concetto di confine statale. I sistemi giuridici nazionali, però, spesso sembrano ignorare tale natura.

Invero, lo spazio informatico è – come osservato – uno spazio globale e tendenzialmente refrattario alle limitazioni nazionali. Con la diffusione delle tecnologie informatiche e del *web* si è sviluppata una nuova area trascendente il tradizionale rapporto basato sulla fisicità spazio-temporale che ha posto in crisi il tradizionale concetto di sovranità degli ordinamenti e la loro pretesa di regolare i fatti manifestatisi sul proprio territorio²⁶³.

Secondo la dottrina, la natura transnazionale della prova digitale si caratterizza per tre aspetti: localizzazione e conservazione della prova digitale; sede dell'*Internet Service Provider*; natura transnazionale del presunto crimine. A ciò si aggiunga la necessità di accordi interstatuali per lo scambio della prova²⁶⁴.

Ed invero, la prova digitale può essere conservata in qualunque parte del mondo e può riguardare qualsiasi tipologia di reato. Inoltre, le prove digitali spesso derivano da fonti private. L'accesso e il possesso di tali informazioni utili per il processo sono riservati agli *Internet Service Provider*, i quali spesso non hanno la propria sede nello stesso Stato dove il reato per cui si richiede la prova è perseguito. Infine, non va sottovalutato che per alcuni reati, fenomenicamente, spesso sono coinvolte più giurisdizioni, con evidente difficoltà relativa alla formazione, conservazione e spendibilità nel processo delle informazioni raccolte.

La natura digitale dell'informazione, le moderne tecnologie e la galoppante globalizzazione hanno fluidificato la prova, la quale spesso sfugge alla sovranità dello Stato dove il reato è perseguito. La situazione si complica se si tiene conto dell'attuale difficoltà della cooperazione giudiziaria internazionale di rispondere a nuove esigenze quali la formazione della prova in luoghi totalmente virtuali quali ad esempio il *cloud*²⁶⁵.

²⁶³ In tal senso, F. SIRACUSANO, *Prove informatiche*, cit., p. 254 ss.

²⁶⁴ Così, M.A. BIASIOTTI, S. CONTI, F. TURCHI, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, cit., p. 1641 ss.

²⁶⁵ Il Consiglio d'Europa, nell'ambito del gruppo di lavoro sulla *Cybercrime Convention* (T-CY), nella sua XII Sessione plenaria del 2-3 dicembre 2014, ha affrontato la questione dello scambio della prova elettronica nella sua prospettiva più spinosa, ossia quella relativa all'acquisizione della prova elettronica dal *cloud* creando un apposito gruppo di lavoro – il *Cloud Evidence Group* – il quale ha il compito di studiare quali soluzioni possano essere adottate per garantire alla giustizia penale l'accesso alle prove conservate in ambienti *cloud*, comprese le soluzioni che possono essere compatibili con le procedure di

I confini statuali diventano evanescenti perché possono essere superati dal mondo virtuale. L'approccio esclusivamente nazionale al tema risulta inadeguato poiché la criminalità ormai appare sempre più "liquida" proprio grazie alla sua dimensione sempre più transnazionale, capace di colpire a livello globale usando un solo dispositivo informatico ma senza avere un'organizzazione strutturata a sostegno²⁶⁶.

Con la diffusione del *cloud computing* si assiste, infine, alla definitiva difficoltà – o addirittura impossibilità – di plasmare l'acquisizione del dato da acquisire sul concetto di territorializzazione. La localizzazione dei dati può rivelarsi di conseguenza inutile perché, una volta individuato il *service provider* che fornisce il servizio di *cloud computing*, comunque nulla si saprebbe in merito alla effettiva collocazione del dato²⁶⁷.

In alternativa, gli organi investigativi dovrebbero acquisire le prove con mezzi propri – come, ad esempio, il *trojan* – accettando, però, il rischio di danneggiarle o pregiudicarne la genuinità, compromettendone l'utilizzo nel giudizio²⁶⁸.

Sfumano, dunque, i concetti di sovranità, territorialità e giurisdizione che tradizionalmente caratterizzano la cooperazione transfrontaliera. A tal proposito si parla di *loss of location*, in cui i dati e le prove di qualsiasi reato sono dispersi nel *web*, ossia in un luogo non delimitabile territorialmente e rispetto al quale non è possibile individuare con facilità la giurisdizione²⁶⁹.

La nazionalità del dato e la posizione del titolare del suo trattamento rispetto alla richiesta di accesso o di trasmissione avanzata dalle forze investigative o dall'autorità giudiziaria sono aspetti da porre al centro dell'analisi relativa alla formazione della prova in uno spazio di libertà, sicurezza e giustizia quale vuole essere quello europeo. Le criticità emerse attinenti alla territorialità e alla giurisdizione in relazione ai dati provenienti dal *cloud computing*, ai dati gestiti dagli *Internet provider*, nonché a quelli amministrati dai gestori della telefonia mobile vanno prima analizzate e poi eliminate al fine di istituire un sistema realmente efficiente, capace di combattere la criminalità organizzata transnazionale, le cui attività sono condotte sempre più con strumenti tecnologici.

Le informazioni ricavabili sono di evidente utilità per le indagini e nondimeno di difficile acquisizione a causa dei dinieghi e degli ostacoli frapposti dai rispettivi titolari, peraltro spaventati da vuoti normativi della materia che possano coinvolgerli in responsabilità relative alla lesione di diritti fondamentali²⁷⁰.

assistenza reciproca. Sul *Council of Europe Cybercrime Programme*, M.A. BIASIOTTI, *Presente e futuro dello scambio della prova elettronica in Europa*, in *Informatica & diritto*, 1-2, 2015, p. 50.

²⁶⁶ Così, F. CAJANI, *Interception of communications: Skype, Google, Yahoo! And Microsoft tools and electronic data retention on foreign servers: A legal perspective from a prosecutor conducting an investigation*, in *Digital Evidence and Electronic Signature Law Review*, 6, 2009, p. 158 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 167; F. SIRACUSANO, *La prova informatica transnazionale: un difficile «connubio» fra innovazione e tradizione*, in *Proc. pen. e giust.*, 1, 2017, p. 178 ss.

²⁶⁷ Con il *cloud computing* i dati sono salvati direttamente su *Internet*, e spesso sono spostati dal gestore da un *server* all'altro, per esigenze organizzative, tecniche o economiche (cosiddette *load balancing*). Anche lo stesso utilizzatore non si collega sempre al medesimo *server* per accedere ai propri dati. In questi termini, F. SIRACUSANO, *Prove informatiche*, cit., p. 252 ss.

²⁶⁸ In tal senso, V.L. BARTOLI, *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *Big data and Public Law: new challenges beyond data protection*, in *rivista.eurojus.it*, num. spec., 2019, p. 102.

²⁶⁹ Così, F. SIRACUSANO, *Prove informatiche*, cit., p. 253.

²⁷⁰ Sul punto, C. ASARO, *Sul cammino tracciato da Evidence*, cit., p. 142.

Il quadro normativo sulla prova digitale nel contesto della cooperazione giudiziaria in materia penale con cui si trovano ad operare le autorità di polizia e quelle giudiziarie ancora oggi è notevolmente incerto. Generalmente, l'ambito relativo alla cooperazione giudiziaria penale si presenta intricato, nodoso, ove è difficile orientarsi a causa di un dedalo normativo fatto di convenzioni bilaterali, accordi multilaterali, direttive e regolamenti che convivono tra loro e con le norme del diritto internazionale generale.

Si è avuta così una forte stratificazione normativa: vi sono convenzioni che regolano i rapporti con i Paesi extraeuropei e quelle che regolano i rapporti con Paesi europei. Tra i Paesi europei vi è da distinguere i rapporti con i Paesi che fanno parte del Consiglio d'Europa e i Paesi che fanno parte dell'Unione europea e, tra gli stessi Stati membri dell'Unione devono distinguersi quelli dell'Area Schengen, i quali seguono un'ulteriore e diversa disciplina.

A ciò si aggiunga l'inesistenza di un quadro giuridico omogeneo tra i vari Stati membri dell'Unione europea relativo alla formazione, conservazione e scambio di prove digitali, vera e propria sfida del futuro. I mezzi tradizionali per la cooperazione internazionale in materia penale per la lotta alla criminalità non sono più sufficienti, in ragione della particolare natura delle prove elettroniche²⁷¹.

Da qui il tentativo di creare strumenti comuni basati sul principio del mutuo riconoscimento che consenta con maggior celerità rispetto all'ordine europeo di indagine di formare una prova elettronica custodita o in possesso di un *service provider* con sede in un altro Stato membro, garantendo al tempo stesso la genuinità e l'integrità delle prove elettroniche: gli ordini europei di produzione e conservazione.

Un'armonizzazione della disciplina deve, in ogni caso, tener conto di alcune circostanze quali la veloce evoluzione delle tecnologie forensi; l'ammissibilità delle prove digitali nello Stato membro di emissione; la globalizzazione del crimine²⁷². Del resto, non possono essere solo i tradizionali principi della cooperazione giudiziaria a orientare le attività degli organi di indagine, ma anche l'evoluzione tecnologica, capace di abbattere le barriere della sovranità nazionale²⁷³.

È necessaria una stretta collaborazione tra forze di polizia ed autorità giudiziarie degli Stati membri, nel pieno rispetto dei diritti fondamentali della persona²⁷⁴, previo sviluppo di normative comuni attente ad evitare che la prova digitale sia modificata, alterata, cancellata. Ciò è realizzabile anche attraverso *standard* o linee guida comuni che provino ad arginare l'obsolescenza delle tecniche utilizzate per l'estrazione degli elementi di prova digitale. Non va però dimenticato che, all'interno dell'Europa convivono differenti tradizioni per quanto riguarda le fonti del diritto penale sostanziale e processuale²⁷⁵.

Ed invero, spesso si assiste a rischi per la formazione e la conservazione dei dati digitali a causa di pratiche di acquisizione non corrette, dovute non solo alla difficoltà

²⁷¹ In tal senso, M.A. BIASIOTTI, *Presente e futuro dello scambio della prova elettronica in Europa*, cit., p. 52.

²⁷² Cfr., M.A. BIASIOTTI, S. CONTI, F. TURCHI, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, cit., p. 1641 ss.; S. CONTI, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica & diritto*, 1-2, 2015, p. 153 ss.

²⁷³ In questi termini, F. SIRACUSANO, *Prove informatiche*, cit., p. 256.

²⁷⁴ Il diritto di difesa della persona sottoposta ad indagini o imputata, il diritto alla riservatezza, la tutela dei dati personali, la legalità delle procedure investigative e di acquisizione della prova.

²⁷⁵ Così, E.J. KOOPS, T. ROBINSON, *Cybercrime Law: A European Perspective Crime*, in E. CASEY (ed.), *Digital Evidence and Computer Crime*, III ed., Waltham, 2011, p. 123 ss.

nell'esecuzione stessa delle attività, ma anche a causa dell'adozione di procedure e *standard* disomogenei adottati nei vari Stati²⁷⁶.

Interpreti di tali esigenze sono e dovranno essere il Consiglio d'Europa e l'Unione europea, i quali hanno influenzato ed ancora oggi influenzano le legislazioni nazionali in materia di crimini informatici e di formazione, conservazione e trasferimento delle prove digitali. Con la loro azione, è possibile creare un *humus* normativo comune necessario per realizzare un'armonizzazione legislativa tra i vari Stati membri e con i Paesi terzi.

La Commissione europea nel 2019 ha notato che «le prove elettroniche sono necessarie per circa l'85% delle indagini penali, e per due terzi di queste indagini vi è la necessità di ottenere tali prove da prestatori di servizi online con sede in un'altra giurisdizione. Il numero di richieste trasmesse ai principali prestatori di servizi online è aumentato dell'84% tra il 2013 e il 2018»²⁷⁷. Il 65 % delle richieste totali è rivolto a prestatori con sede in un'altra giurisdizione²⁷⁸.

Il Consiglio europeo Affari interni e Giustizia del 9 giugno 2016 ha identificato nelle sue conclusioni tre azioni per il miglioramento della giustizia penale in Europa:

«– la razionalizzazione delle procedure di assistenza giudiziaria reciproca e, ove applicabile, di mutuo riconoscimento relativamente al ciberspazio grazie all'uso di moduli e strumenti elettronici standardizzati;

– il miglioramento della cooperazione con i fornitori di servizi attraverso lo sviluppo di un quadro comune (es. uso di moduli e strumenti allineati) per richiedere specifiche categorie di dati;

– l'avvio di un processo di riflessione su possibili criteri di collegamento per la competenza esecutiva nel ciberspazio».

In particolare, i ministri hanno tenuto un dibattito orientativo sulle seguenti questioni:

«– i possibili criteri di competenza esecutiva applicabili nel ciberspazio, ad es. i criteri secondo cui le autorità pertinenti possono compiere un atto d'indagine nel ciberspazio quando non sono sufficienti i quadri esistenti, come nei casi in cui le prove elettroniche pertinenti sono nascoste o si spostano velocemente tra le giurisdizioni e

²⁷⁶ Tali circostanze possono indurre la criminalità più attenta ad elaborare tecniche di contrasto alle indagini, privilegiando l'utilizzo dei *server* collocati in Stati poco sensibili ai temi della cooperazione giudiziaria. A ciò si aggiunga la circostanza che la criminalità tende sempre più a commettere reati o a frazionare la condotta criminosa in modo da coinvolgere una molteplicità di Stati, nella consapevolezza della difficile conduzione di indagini internazionali, le quali incontrano ostacoli di ordine giuridico. Sovente nel condurre indagini informatiche risulta fondamentale acquisire l'indirizzo IP utilizzato per la commissione del reato. Proprio tale elemento spesso rappresenta un "pomo della discordia", perché difficilmente conoscibile dagli investigatori a causa della mancanza di cooperazione tra Stati esteri, i quali spesso non rispondono alle richieste, paralizzando l'azione investigativa. In tal senso, N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, in *International Journal of Cyber Criminology*, 1-2, 2010, p. 700; F. SANTORO, *Cooperazione internazionale in materia di criminalità informatica*, Roma, 2011; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 159.

²⁷⁷ Così la Raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione Europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale [COM (2019) 70 final]. Cfr., anche, Comunicazione della Commissione sulla strategia dell'UE per l'Unione della sicurezza [COM (2020) 605 final].

²⁷⁸ Cfr. Commission staff working document impact assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (SWD/2018/118 final).

– un trattamento differenziato di specifiche categorie di dati nei procedimenti penali, ad es. le ripercussioni di un approccio differenziato – tra i dati che non si riferiscono al contenuto (relativi agli abbonati o al traffico) e i dati di contenuto oppure tra i dati in tempo reale e quelli memorizzati – sui singoli quadri giuridici nazionali, il tipo di elementi che sarebbero pertinenti ai fini di un approccio comune a livello di Ue e le misure da prendere in considerazione»²⁷⁹.

Dopo aver provveduto ad un inquadramento sociale, economico e giuridico dell'attuale contesto, che vede lo sviluppo delle nuove tecnologie e la forte predominanza del mondo digitale, e chiarita la natura transnazionale dell'*e-evidence*, è necessario concentrare l'attenzione sugli strumenti presenti e futuri sviluppati nell'ambito della cooperazione giudiziaria in materia penale per l'acquisizione della prova digitale.

In particolare, oggetto di analisi saranno gli strumenti attualmente esistenti e in via di formazione, la cui funzione consiste nell'acquisizione da parte di un'autorità di emissione di dati elettronici conservati all'estero da un *internet service provider*.

In tal senso, ci si chiede se gli strumenti già esistenti si siano rivelati efficaci e perché gli ordinamenti statuali e i prestatori di servizi hanno reagito innanzi ai vuoti normativi con la *voluntary disclosure* in attesa di una disciplina più efficiente. Oggetto di valutazione sono gli strumenti della cooperazione giudiziaria specificamente dedicati, analizzati considerando il rapporto tra autorità e libertà, al fine di stabilire se riescono a garantire un equilibrio tra le esigenze contrapposte, rappresentate da un lato dagli interessi alla repressione dei reati ed alla sicurezza internazionale ed interna, dall'altro dall'interesse dei singoli al rispetto dei diritti fondamentali coinvolti nelle attività di acquisizione dei dati elettronici.

Lo studio approfondisce anche l'attività dell'Unione europea nella creazione di strumenti di ultima generazione. Ulteriore obiettivo è capire se è stato avviato un progressivo abbandono del principio di territorialità, se vi sia una sovrapposizione tra strumenti e se l'eccessiva produzione normativa non rischi di rendere caotico il contesto in cui opereranno le autorità giudiziarie.

A tal fine, il lavoro si compone di cinque capitoli. Un primo capitolo, avente lo scopo di spiegare l'attualità dell'indagine ed il contesto sociale in cui si è sviluppata l'esigenza di strumenti per l'acquisizione della prova elettronica transnazionale; un secondo capitolo, utile a tracciare i principi strutturali su cui si regge la cooperazione giudiziaria in materia penale, che faranno da cornice agli strumenti per l'acquisizione della formazione della prova elettronica; un terzo capitolo, che analizza nello specifico gli strumenti a carattere internazionale; un quarto capitolo, con il quale si approfondiscono gli strumenti dell'Unione europea; un ultimo capitolo, ove si trarranno le conclusioni del lavoro, a seguito dello studio dei dati raccolti.

La struttura del lavoro è frutto di un'attenta analisi delle fonti e della disciplina dedicata al tema. Come emergerà nel corso della lettura, il quadro normativo sulla circolazione transnazionale delle prove elettroniche è fortemente variegato, tanto da rendere necessaria una sistematizzazione ed una trattazione specifica di ogni singolo istituto, in modo da far emergere la difficoltà sia dell'interprete sia degli operatori nella ricostruzione delle fonti e nella scelta dello strumento più idoneo al caso concreto per l'acquisizione del dato richiesto. In merito, bisogna sin da subito chiarire che già dal

²⁷⁹ COUNCIL OF EUROPE, *Conclusioni del Consiglio sul miglioramento della giustizia penale nel ciberspazio*, 9 giugno 2016, in www.consilium.europa.eu/it/press/press-releases/2016/06/09-criminal-activities-cyberspace.

principio ci si imbatte in una elefantiaca produzione che ne rende estremamente difficile una ricostruzione.

È, dunque, adoperato un rigido approccio metodologico basato sull'interpretazione sistematica degli istituti, letti sotto la lente di ingrandimento della tutela dei diritti fondamentali temperati mediante l'applicazione dei principi di ragionevolezza e di proporzionalità, alla ricerca di un delicato equilibrio tra valori contrapposti.

Il metodo adottato, basato sull'analisi sistemica e non frazionata delle norme – altrimenti non coordinate ed in potenziale conflitto tra loro²⁸⁰ –, vuole tendere ad una operazione di moderazione e ponderazione degli interessi e dei diritti contrapposti. Attraverso il prisma della ragionevolezza e della proporzionalità si anela all'analisi degli istituti, dilatando i canoni logico-razionali, nella consapevolezza dell'intrinseca imperfezione della giustizia e nell'aspirazione all'evoluzione ed al confronto giuridico²⁸¹.

Teleologia ed assiologia saranno gli elementi che guideranno l'analisi degli strumenti, alla ricerca di possibili vuoti normativi o imperfezioni del sistema in corso di formazione dedicato all'acquisizione delle prove elettroniche transnazionali.

Dopo il primo capitolo, in cui è stato illustrato lo spazio ed il tempo del “mondo digitale”, è stata definita la prova elettronica ed è stato chiarito come l'esplorazione in un mondo ancora particolarmente ignoto per il settore legale sia attività spinosa, il lavoro prosegue (secondo capitolo) con la trattazione dei principi strutturali della cooperazione giudiziaria in materia penale: la mutua assistenza ed il mutuo riconoscimento. I due principi rappresentano la premessa necessaria da cui partire per l'analisi degli strumenti destinati all'acquisizione dell'*e-evidence*.

In particolare, con il capitolo si tracciano le loro caratteristiche, evidenziandone luci ed ombre e chiarendo l'azione ed il ruolo dell'Unione europea verso una evoluzione del principio del mutuo riconoscimento. Inoltre, si indicheranno anche le peculiarità del principio di equivalenza e del principio di proporzionalità. I principi, utilizzati anche per la produzione normativa, rappresentano i mezzi ermeneutici necessari nella scelta dello strumento più adeguato al caso concreto.

Il terzo capitolo è dedicato al contesto internazionale. In particolare, oggetto di trattazione saranno gli strumenti creati con la Convenzione europea sulla criminalità informatica ed il relativo Secondo protocollo nonché la normativa statunitense di recente introdotta con il *CLOUD Act*.

Al quadro generale relativo alla Convenzione europea sulla criminalità informatica – in cui si presta attenzione anche al contesto storico in cui si è sviluppata – succede la rassegna degli strumenti della mutua assistenza per la formazione dell'*e-evidence*, ove si chiarirà come questi si siano rivelati nel tempo inefficaci e come la normativa risulti poco chiara e precisa, tanto da aver richiesto periodiche spiegazioni che, tuttavia, non hanno sortito l'effetto di migliorare ed accelerare le attività finalizzate all'acquisizione delle prove elettroniche transnazionali.

L'inefficacia e la lentezza degli strumenti hanno indotto il Consiglio d'Europa a redigere un Secondo protocollo alla Convenzione, che proponesse agli Stati un ventaglio di nuovi strumenti che garantiscono (almeno nelle intenzioni) la celerità ed il conseguimento degli obiettivi.

Dopo aver delineato le caratteristiche dei nuovi strumenti “a più velocità” creati dal Consiglio d'Europa in relazione al tipo di dato elettronico e fatto emergere elementi di

²⁸⁰ Cfr., Corte cost., sentenza del 9 maggio 2013, n. 85, in *Giur. Cost.*, 3, 2013, p. 1424 ss.

²⁸¹ In argomento, M. CARTABIA, *Edipo Re*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), Bologna, 2018, p. 54 ss.

frizione e dubbiose tecnicità, l'attenzione si concentrerà sul *CLOUD Act*, sulla sua genesi e sulle attività ancora in corso tra Stati Uniti d'America e Unione europea per la redazione di un Accordo esecutivo che consenta ai Paesi membri di richiedere direttamente ai prestatori di servizi presenti sul territorio statunitense l'acquisizione dei dati elettronici in loro possesso. Particolarmente interessante sarà scoprire se l'Unione europea sarà capace di compiere un'opera di persuasione per raggiungere uno *standard* adeguato di tutela dei diritti fondamentali non solo per le richieste *agli* Stati Uniti, ma anche per le richieste *dagli* Stati Uniti, dal momento in cui per queste ultime non appare necessario un Accordo esecutivo.

Il quarto capitolo approfondirà gli strumenti sviluppati dall'Unione europea. Dapprima, si spiegherà come l'ordine europeo di indagine, seppur ha mostrato un miglioramento nei rapporti tra autorità ed accelerato i tempi per la formazione delle prove, risulti inadeguato per le attività attinenti all'acquisizione di dati elettronici. Successivamente, si illustrerà il percorso compiuto per la creazione di strumenti all'avanguardia basati sul principio del mutuo riconoscimento: l'ordine europeo di conservazione e l'ordine europeo di produzione.

Nel descrivere la disciplina attualmente all'attenzione del decisore europeo, si proverà ad evidenziare gli aspetti positivi e le zone d'ombra, alla luce della tutela dei diritti fondamentali, al fine di ricercare un difficile equilibrio tra i diritti coinvolti, lasciando emergere con chiarezza le difficoltà riscontrabili per la normazione di strumenti particolarmente intrusivi della riservatezza delle persone.

Nel fare sintesi, le conclusioni si concentreranno sugli aspetti innovativi degli strumenti e sulle linee evolutive tracciate a livello internazionale ed europeo, come ad esempio il rapporto diretto tra autorità pubblica e società privata. Inoltre, si sottolineerà la necessità di un approccio pragmatico ai temi proposti e si proverà a persuadere il lettore della necessità di agire in tempi celeri per aggredire le nuove forme di criminalità nel contesto digitale, cercando di delineare proposte che rappresentino il frutto di un bilanciamento tra valori contrapposti e lasciando emergere alcune criticità.

Le riflessioni che si proporranno nascono da precise domande volte a sondare i profili evolutivi ed i nuovi principi su cui si baseranno gli strumenti per la formazione dell'*e-evidence*, tentando di dare una lettura del futuribile. Non mancherà di rimarcare come le nuove regole in tema di acquisizione di prove elettroniche rappresentino un vero cambio di passo, una rottura degli schemi, un'apertura a principi di nuova generazione.

In particolare, bisognerà comprendere in che modo i principi della mutua assistenza e del mutuo riconoscimento possono agire nel rapporto diretto tra le autorità pubbliche di uno Stato e i prestatori di servizi stanziati in un altro Stato e come tale rapporto tenderà a far evolvere la cooperazione giudiziaria in materia penale in una direzione sinora inesplorata, verso scenari futuri che potrebbero cambiare i rapporti internazionali ed il volto dell'Unione europea, mediante una maggior coesione degli Stati membri ed una apertura alla forma federale.

Pertanto, è necessario un preliminare approfondimento sui due principi strutturali della mutua assistenza e del mutuo riconoscimento.

CAPITOLO II

COOPERAZIONE GIUDIZIARIA IN MATERIA PENALE E MUTUO RICONOSCIMENTO

Sommario: 1. La “sfida” della cooperazione giudiziaria in materia penale. – 1.1. (Segue). La “quinta libertà” e la cooperazione giudiziaria come esigenza. – 2. La disciplina della cooperazione giudiziaria in materia penale nell’Unione europea. – 3. (Segue). La cooperazione “verticale” e la cooperazione “orizzontale”. – 4. Le nuove sfide e gli sviluppi della cooperazione giudiziaria in materia penale nell’Unione europea. – 5. Il principio della mutua assistenza e la progressiva riduzione della sua applicazione. – 6. Il principio cardine della cooperazione giudiziaria tra Stati membri dell’Unione europea: il mutuo riconoscimento. – 7. Il mutuo riconoscimento quale presupposto per la “libera circolazione” delle decisioni giudiziarie. – 8. La “fiducia reciproca” e il rispetto dei diritti fondamentali quali elementi necessari per il mutuo riconoscimento. – 9. Il principio del mutuo riconoscimento tra uniformazione e armonizzazione. – 10. L’inclusione del principio del mutuo riconoscimento nel Codice di procedura penale italiano. Il titolo I-*bis* del Libro XI del Codice di rito. – 11. (Segue). La formulazione del nuovo art. 696-*bis* c.p.p. – 12. Il principio di equivalenza e il principio di proporzionalità nel sistema dell’Unione europea. 13. L’attenzione dell’Unione europea al tema della prova elettronica. – 14. (Segue). Verso nuovi strumenti per la formazione della prova elettronica transnazionale.

1. La “sfida” della cooperazione giudiziaria in materia penale

Come è noto, per “cooperazione internazionale in materia penale” si intende l’attività di collaborazione internazionale nella lotta contro il crimine²⁸². Nel definirla, c’è chi ha utilizzato l’immagine di una cerniera tra il diritto interno e quello internazionale²⁸³.

Con la nascita delle Comunità europee prima e dell’Unione Europea poi, si è avvertita forte l’esigenza di creare un apparato comune di norme ed istituzioni volte a contrastare le varie forme di criminalità di stampo transnazionale.

²⁸² P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 1097 ss. L’autore sottolinea come la cooperazione internazionale in materia penale abbia avuto un eccezionale sviluppo a partire dal secondo dopoguerra a causa dello sviluppo di forme di criminalità che hanno giustificato la creazione di strumenti convenzionali a carattere multilaterale. V., inoltre, A. GAITO, *Spazio penale europeo e cooperazione giudiziaria internazionale*, in AA.VV., *Procedura penale*, Torino, 2019, p. 973 ss.

Sul tema si veda anche, *ex multis*, M. BARGIS, *La cooperazione giudiziaria penale nell’Unione europea tra mutuo riconoscimento e armonizzazione: analisi e prospettive*, in *Riv. Dir. Proc.*, 4, 2012, p. 914 ss.; G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all’ordine di indagine*, Milano, 2017; L. CAMALDO, F. MANFREDINI, *La cooperazione giudiziaria nell’era delle minacce globali e la riforma del libro XI del codice di procedura penale*, in *Cass. Pen.*, 7/8, 2016, p. 3043B ss.; M. CHIAVARIO, *Diritto processuale penale*, Torino, 2015, p. 908 ss.; ID., *Cooperazione giudiziaria e di polizia in materia penale a livello europeo*, in *Riv. It. Dir. Proc. Pen.*, 3, 2005, p. 974 ss.; S. CIVELLO CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell’Unione Europea*, in *penalecontemporaneo.it*, 3 giugno 2013; G. DE AMICIS, *Prevalenza del diritto dell’Unione europea, delle convenzioni e del diritto internazionale in generale*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 3 ss.; A. DI STASI, *Spazio europeo di libertà, sicurezza e giustizia e cooperazione giudiziaria in materia penale: il rispetto dei diritti fondamentali e della diversità tra ordinamenti nazionali e tradizioni giuridiche*, in «Spazio europeo di giustizia» e *procedimento penale italiano* (a cura di L. KALB), cit., p. 3 ss.; F. FALATO, *Appunti di cooperazione giudiziaria penale*, Napoli, 2019; V. MITSILEGAS, *EU Criminal Law After Lisbon: Rights, Trust and the Transformation of Justice in Europe*, Oxford, 2018; S. MONTALDO, *I limiti della cooperazione in materia penale nell’Unione europea*, Napoli, 2015; S. NEGRI, *L’incidenza della Convenzione europea dei diritti dell’uomo sulla cooperazione giudiziaria penale nell’Unione Europea*, in «Spazio europeo di giustizia» e *procedimento penale italiano* (a cura di L. KALB), Torino, 2012, p. 55 ss.; L. PALMIERI, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, Milano, 2019; T. RAFARACI, *Lo spazio di libertà, sicurezza e giustizia nel crogiolo della costruzione europea*, in AA.VV., *L’area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007, p. 33 ss.; A. SCALFATI, *Note minime su cooperazione investigativa e mutuo riconoscimento*, in *Proc. pen. e giust.*, 2, 2017, p. 217 ss.; F. SPIEZIA, *La cooperazione giudiziaria internazionale e lo spazio di giustizia europeo*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), IV, *Le impugnazioni. Esecuzione penale. Rapporti giurisdizionali con autorità straniere* (a cura di L. KALB), Torino, 2015, p. 815 ss.; A.M. STILE, *The Instruments of the Former third pillar in the Lisbon era: towards an Integral Judicial Control in the Area of Security, Liberty and Justice*, cit., p. 482 ss.; G. TIBERI, *Le nuove fonti del diritto nella cooperazione giudiziaria in materia penale dopo il Trattato di Lisbona e il loro impatto sull’ordinamento interno*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell’Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), Milano, 2011, p. 13 ss.; A. WEYEMBERGH, *Storia della cooperazione*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 207 ss.; E. ZAPPALÀ, F. SIRACUSANO, *I rapporti giurisdizionali con autorità straniere*, in AA.VV., *Diritto processuale penale* (a cura di G. DI CHIARA, V. PATANÈ, F. SIRACUSANO), Milano, 2013, p. 917 ss.

²⁸³ Così, C. STORTI, *La Rogatoria Internazionale nei Codici dell’Unificazione Italiana (1861-1930)*, in AA.VV., *Atti del VII Convegno di Studi – La circolazione della prova nell’UE e la tutela degli interessi finanziari* (a cura di L. A. BANA, L. CAMALDO), Milano, 2011, p. 23 ss.

La scelta di formare un Mercato europeo comune (MEI)²⁸⁴, basato sulla libera circolazione di persone, merci, servizi e capitali, nonché gli accordi di Schengen²⁸⁵, che eliminano le frontiere interne agli Stati e creano il c.d. “spazio Schengen”, hanno determinato anche lo sviluppo di una criminalità “a carattere europeo”, operativa in questo territorio o su parte di esso.

Internet e le nuove tecnologie hanno, infine, dato nuovo impulso a queste forme di criminalità transnazionale. Per tale motivo è necessario prevedere delle misure volte a compensare un *vulnus* di sicurezza dovuto alla maggiore libertà di circolazione.

In realtà, il fenomeno della “criminalità transnazionale”²⁸⁶ si era sviluppato e diffuso già prima della nascita della Comunità Europea o comunque dell’Unione Europea. Si pensi, ad esempio, alla criminalità organizzata italo-americana, alla mafia Russa, alla mafia cinese o ancora ai cartelli colombiani e messicani, caratterizzati da un raggio d’azione sicuramente più ampio dei confini statuali e internazionalmente operative già da vari decenni.

Le organizzazioni regionali, nate con lo scopo di tutelare e promuovere gli ideali e i principi comuni nonché per favorire il loro progresso economico e sociale anche mediante un’integrazione economica basata sull’eliminazione delle restrizioni alla circolazione di persone, beni, servizi e capitali, hanno contribuito allo sviluppo di tale tipologia di criminalità ed hanno spalancato le porte a nuovi tipi di traffici e mercati illegali.

La responsabilità di una capillare diffusione dei fenomeni legati alla criminalità organizzata transnazionale non è, però, di certo attribuibile a tali organizzazioni²⁸⁷. Infatti, la loro attività, internazionalmente meritevole perché a beneficio dei popoli, non poteva fenomenologicamente escludere in alcun modo effetti collaterali spiacevoli, ineliminabili in un contesto simile.

È fisiologico che una apertura dei confini abbia favorito la circolazione più veloce e libera di merci, persone e capitali, ma abbia anche portato con sé, come altra faccia della medaglia, lo sviluppo della criminalità transnazionale. Tale scelta, dettata dall’esigenza di rispondere alle nuove sfide della globalizzazione e di conseguire il maggior benessere possibile per la popolazione, ha fatto sorgere esigenze quali la lotta a nuove forme di

²⁸⁴ Il Mercato europeo comune viene realizzato con i Trattati di Roma firmati il 25 marzo 1957, entrati in vigore il 1° gennaio 1958. Per il testo completo dei trattati si rimanda al sito <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:11957E/TXT>.

²⁸⁵ La Convenzione di Schengen venne firmata il 19 giugno 1990 da Francia, Repubblica federale della Germania (Germania ovest) e i governi degli Stati dell’Unione Economica del Benelux (Belgio, Paesi Bassi e Lussemburgo). Alla convenzione hanno in seguito aderito anche Italia (1990), Spagna e Portogallo (1991), Grecia (1992), Austria (1995), Danimarca, Finlandia e Svezia (1996). Lo Spazio Schengen si è poi progressivamente allargato a quasi tutti gli Stati membri e a molti Stati non membri dell’UE.

²⁸⁶ L’espressione criminalità transnazionale viene utilizzata per la prima volta in occasione della *Naples Political Declaration on Global Action Plan against Organized Crime* nei lavori dell’ONU (doc. A/49/748). La dichiarazione è frutto della Conferenza ministeriale sul crimine organizzato tenutasi dal 21 al 23 novembre 1994 a Napoli. Da tale momento in poi il termine comparirà regolarmente nei documenti ufficiali, e segnatamente nei lavori preparatori che confluiranno nella Convenzione di Palermo del 2000, la quale all’art. 3, par. 2, definisce in modo chiaro il reato di criminalità transnazionale. Per un’ampia trattazione del tema si rimanda a E. ROSI (a cura di), *Criminalità organizzata transnazionale e sistema penale italiano. La convenzione ONU di Palermo*, Roma, 2007. Per un approfondimento sul rapporto tra criminalità e globalizzazione si veda anche R. SCIARRONE, *Processi di globalizzazione e criminalità organizzata*, in AA.VV., *Potere politico e globalizzazione* (a cura di P. FANTOZZI), cit., p. 175 ss.

²⁸⁷ Si pensi all’istituzione dell’Unione Europea, dell’OSA (Organizzazione degli Stati Americani), del NAFTA (Accordo di Libero Scambio Nordamericano), il MERCOSUR (Mercato Comune del Sud), dell’ASEAN (Associazione delle Nazioni dell’Asia Sud-Orientale), dell’APEC (Asia-Pacific Economic Cooperation), dell’UA (Unione Africana).

criminalità attraverso la creazione di strumenti innovativi basati sulla cooperazione giudiziaria come, ad esempio, le rogatorie, cioè richieste rivolte da uno Stato ad un altro per ottenere lo svolgimento di determinate attività sul territorio estero al fine di raggiungere dei risultati utili per le indagini o per il processo²⁸⁸.

Accanto a una integrazione di tipo economico, si sono sviluppate forme di cooperazione in materie dove era forte in passato il rispetto del principio della sovranità statale²⁸⁹. Ciò è stato possibile perché la tutela delle nuove esigenze di sicurezza e difesa sociale è stata avvertita come superiore rispetto alla “santificazione” del principio di sovranità statale²⁹⁰.

Tali esigenze sono volte a neutralizzare il pericolo di diffusione e di operatività di un tipo di criminalità che spesso risulta essere *borderline* poiché assume la forma di società finanziarie o commerciali che nascondono operazioni di riciclaggio di denaro sporco o acquistano un ruolo primario anche nel campo del traffico di sostanze stupefacenti. Infine, forte impulso è stato dato dai nuovi pericoli come il terrorismo internazionale.

Orbene, l’esigenza di combattere queste nuove manifestazioni di criminalità – che spesso si avvalgono anche di sofisticati strumenti tecnologici – ha spinto gli Stati ad abbandonare le proprie posizioni di chiusura e di conservatorismo per avviare lo sviluppo di nuovi e più avanzati modelli di cooperazione attraverso “*l’internazionalizzazione della repressione*”²⁹¹, ossia l’instaurazione di forme sempre più incisive di collaborazione giudiziaria e di polizia tra Stati tali da prevenire, evitare o comunque limitare ovvero reprimere la criminalità.

Alla luce di ciò, è necessario rivedere il concetto di cooperazione giudiziaria poiché risulta indispensabile abbandonare le valutazioni di opportunità politica e superare la visione tradizionale di essa come tecnica di affermazione della sovranità statale e come strumento di protezione degli interessi pubblicistici del singolo Stato in modo da abolire quegli strumenti di cooperazione ormai obsoleti e inefficaci ancorati a meccanismi politici che irrigidiscono le procedure, così da combattere la “globalizzazione della criminalità” con la “globalizzazione della legalità”²⁹².

²⁸⁸ Sul punto, P. SPAGNOLO, *La Nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, in *Cass. pen.*, 3, 2020, p. 1291, secondo la quale «la globalizzazione ha consentito il superamento delle tradizionali frammentazioni, con effetti sia positivi – per quanto interessa al nostro tema, gli Stati da monadi isolate sono diventati Stati membri e i cittadini del vecchio mondo, cittadini europei – sia negativi, con il progressivo affermarsi della criminalità transfrontaliera».

²⁸⁹ In argomento, si veda G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «*Spazio europeo di giustizia*» e *procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012, p. 503 ss., il quale nota come la globalizzazione dei mercati e lo sviluppo di nuove tecnologie informatiche e di comunicazione abbiano creato nuove tipologie di crimini che ledono beni protetti con effetti sostanziali anche in altri Stati.

²⁹⁰ Sul concetto di sovranità, vedi, su tutti, A. DI STASI, *The Enlargement of Competences of the European Union between State Sovereignty and the so-called European “Sovereignty”*: Focus on the limits of Applicability of the Charter of Fundamental Rights of the European Union, in *Araucaria. Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, 3, 2020, p. 131 ss.; M. NINO, *The Evolution of the Concept of Territorial Sovereignty. From the Traditional Westphalian System to the State-Peoples Binomial*, in *La comunità internazionale*, 4, 2020, p. 561 ss.

²⁹¹ Il termine è di F. FALATO, *Appunti di cooperazione giudiziaria penale*, Napoli, 2012, p. 9.

²⁹² In tema, L. CAMALDO, F. MANFREDINI, *La cooperazione giudiziaria nell’era delle minacce globali e la riforma del libro XI del codice di procedura penale*, cit., p. 3043B ss.

Per fare ciò gli Stati hanno attenuato la portata del “principio della sovranità statale”²⁹³ per il quale essi hanno il diritto di esercitare esclusivamente nel proprio territorio il potere – anche coercitivo – su un determinato popolo. L’esclusività della sovranità, non a caso, è espressa in maniera chiara dal famoso brocardo “*rex in regno suo superiorem non recognoscens imperator est*”. Ma come se non bastasse, la dottrina ha sottolineato che tale erosione ha addirittura rovesciato il principio del divieto di ingerenza stabilendo il diritto di interferenza negli affari interni dello Stato consistente in una forma di pretesa da parte delle organizzazioni sovranazionali (comprese l’Unione Europea), fonte di forte limitazione della sovranità²⁹⁴.

In passato, il notevole senso della sovranità degli Stati non ha di fatto bloccato l’avvio e lo sviluppo di forme di cooperazione interstatale, ma ha agevolato il ricorso alla mutua assistenza perché avvertita quale principio per rilanciare e riaffermare la sovranità degli Stati²⁹⁵.

In realtà, gli ordinamenti statuali si sono mostrati a lungo restii nell’accettare e agevolare forme di coordinamento in materia penale in funzione di prevenzione e repressione dei reati di carattere transnazionale, poiché ritenevano che ciò equivallesse a riconoscere o dare la percezione all’esterno di una propria debolezza interna, apparendo non autosufficienti e privi di strumenti necessari per la lotta al crimine.

Col tempo, è diventata preminente l’esigenza di adeguare la normativa interna a quella sovranazionale, relativa al miglioramento ed alla creazione di nuovi strumenti giudiziari di maggiore efficacia nella lotta alla criminalità e di maggior incisività nelle contestuali politiche di sicurezza e garanzia dell’effettività dei diritti fondamentali.

Si pensi, a titolo esemplificativo, alle squadre investigative comuni ovvero al mutuo riconoscimento dei provvedimenti giudiziari o ancora alla circolazione delle informazioni, delle fonti di prova e degli elementi di prova, soprattutto elettronici.

Se da una parte l’esigenza è quella di prevenire e combattere con decisione il crimine dando una risposta concreta alle richieste di sicurezza provenienti dai cittadini, dall’altra si pone l’esigenza di dover approntare strumenti ed istituti della cooperazione basati sul rispetto dei diritti fondamentali che siano al tempo stesso effettivi ed efficaci. In tal senso, è necessario prevedere strumenti di cooperazione che rispettino i diritti fondamentali individuati nella Carta dei diritti fondamentali dell’Unione europea del 7 dicembre 2000²⁹⁶ e sanciti dalla Convenzione per la salvaguardia dei diritti dell’uomo e delle libertà

²⁹³ Così, G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), Napoli, 2020, p. 995.

²⁹⁴ Cfr. S. LABRIOLA, *I fini dello Stato e l’umanità plurale*, in AA.VV., *Ripensare lo Stato* (a cura di S. LABRIOLA), Milano, 2003, p. 93 ss.

²⁹⁵ Sul punto si veda V. ESPOSITO, voce *Rapporti giurisdizionali con autorità straniere*, in *Enc. Giur.*, XXV, Roma, 1991, p. 1 ss.

²⁹⁶ Adattata il 12 dicembre 2007 a Strasburgo, avente lo stesso valore giuridico dei trattati – e dunque rango di fonte primaria – grazie all’espressa previsione dell’art. 6 del Trattato sull’Unione europea come modificato in seguito all’entrata in vigore del Trattato di Lisbona. Per un approfondimento sul valore della Carta dei diritti fondamentali dell’Unione europea e sulla sua applicazione giurisprudenziale, nella smisurata letteratura, v. A. BARBERA, *La Carta dei diritti: per un dialogo fra la Corte italiana e la Corte di giustizia*, in *Quaderni Costituzionali*, 2018, 1, pp. 149-171; G. BISOGNI, G. BRONZINI, V. PICCONE (a cura di), *La Carta dei diritti dell’Unione europea. Casi e materiali*, Taranto, 2009; M. CARTABIA, *L’impatto costituzionale della Carta dei Diritti dell’Unione europea*, in AA.VV., *Liber Amicorum Antonio Tizzano*, Torino, 2018, pp. 179-189; L. DANIELE, *La Carta dei diritti fondamentali dell’Unione europea e il Trattato di Lisbona*, in *Liber Fausto Pocar*, Milano, 2009; S. DE VRIES, E. BERNITZ, S. WEATHERILL (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument*, Abington, 2015; A. DI STASI, *Tutela dei diritti fondamentali e spazio europeo di giustizia*, Napoli, 2019; ID., *L’incidenza virtuosa dei diritti fondamentali*

fondamentali²⁹⁷, così come interpretati dalla Corte di Strasburgo, in modo da assicurare un sistema legale, trasparente, chiaro, garantista, che rispetti il supremo principio del giusto processo²⁹⁸.

Infatti, l'esigenza di una maggior sicurezza ed il contrasto alle gravi forme di reato e di terrorismo non devono causare ingiustificate lesioni delle libertà dei cittadini. Piuttosto, va operato un equo bilanciamento tra esigenze contrapposte a garanzia dello sviluppo armonico della società. D'altra parte, però, è necessario prevedere nuovi strumenti di cooperazione che non siano caratterizzati dalla lentezza, in modo da dare una risposta, se non immediata, quanto meno tempestiva alle nuove minacce globali che si affacciano sullo scenario internazionale.

Inoltre, l'obiettivo della cooperazione giudiziaria è quello di evitare alcune distorsioni del sistema man mano sviluppatesi, come il *forum shopping*, una pratica basata sull'accordo tra le polizie di diversi Stati per attribuire la consumazione di un reato in uno Stato invece di un altro attraverso una *fictio*, con conseguente lesione del principio del *locus commissi delicti* e del principio della naturalità del giudice, ledendo così il giusto processo e il canone della precostituzione del giudice a livello costituzionale ed internazionale²⁹⁹. Tra l'altro, tale pratica può essere utilizzata anche dagli stessi criminali, i quali, eludendo le regole e con alcuni espedienti, possono ottenere che il processo di

nel completamento dello Spazio europeo di giustizia, in *Freedom security & justice Review*, 1, 2019, pp. 1-10; ID., *Spazio europeo di libertà, sicurezza e giustizia e cooperazione giudiziaria in materia penale: il rispetto dei diritti fondamentali e della diversità tra gli ordinamenti nazionali e tradizioni giuridiche*, in AA.VV., «*Spazio europeo di giustizia*» e *procedimento penale italiano* (a cura di L. KALB), cit., pp. 3-54. N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Bologna, 2018; S. MANACORDA, «*Doppia pregiudizialità*» e *Carta dei diritti fondamentali: il sistema penale al cospetto del diritto dell'Unione europea nell'era del disincanto*, in *Riv. it. dir. e proc. pen.*, 2, 2020, p. 572 ss.; AA.VV., *Carta dei Diritti Fondamentali dell'Unione Europea* (a cura di R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI), Milano, 2017; S. PEERS, T. HERVEY, S. KENNER, A. WARD (eds.), *The EU Charter of Fundamental Rights. A Commentary on the European Union Charter of Fundamental Rights*, Oxford, 2014; AA.VV., *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività* (a cura di V. PICCONE, O. POLLICINO), Napoli, 2018; K. STERN, *La Carta dei diritti fondamentali dell'Unione europea. Riflessioni sulla forza vincolante e l'ambito di applicazione dei diritti fondamentali codificati nella Carta*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 6, 2014, pp. 1235-1260.

²⁹⁷ La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) è stata adottata nell'ambito del Consiglio d'Europa. Il Consiglio d'Europa è un'organizzazione internazionale con sede a Strasburgo nata nel 1949 al fine di tutelare i principi dello Stato di diritto, libertà politica e diritti umani mediante l'adozione di convenzioni internazionali. Per un approfondimento, sul punto si veda, *inter alia*, A. DI STASI, *Introduzione alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Milano, 2018.

²⁹⁸ In tal senso è da guardare con favore allo sforzo che compiono gli ordinamenti per attuare le direttive europee che garantiscono i diritti fondamentali così come sanciti dalla Carta dei diritti fondamentali dell'Unione europea e dalla CEDU. Si noti come sempre più spesso la dottrina e la giurisprudenza nazionale valorizzino le decisioni della Corte EDU alle quali lo Stato ha l'obbligo di conformarsi. Grazie a questo lavoro di osmosi e di continuo dialogo tra ordinamento interno e ordinamento sovranazionali può realizzarsi non solo un avvicinamento delle legislazioni, ma anche un serio ed effettivo rispetto dei diritti umani. D'altra parte, ciò è anche utile a quell'importante opera di bilanciamento tra contrapposte esigenze che si rinvergono non solo nel campo del diritto penale. Per una raccolta e relativi commenti alle più recenti sentenze nei confronti dell'Italia della Corte europea dei diritti dell'uomo, A. DI STASI, *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno (2016-2020)*, II ed., Milano, 2020.

²⁹⁹ Nell'ordinamento italiano, per il principio della naturalità del giudice si veda l'art. 25 Cost., mentre per il principio del giusto processo si veda l'art. 111 Cost. Per quanto riguarda il principio del *locus commissi delicti* si rimanda all'art. 8 c.p.p. e all'art. 6 c.p.

radichi in fori dove la legge penale è sicuramente più vantaggiosa, o dove è più semplice sottrarsi alla giustizia.

Il *forum shopping* era avvertito come un ostacolo alla cooperazione giudiziaria. Infatti, è possibile individuare non solo frontiere fisiche, ma anche e soprattutto frontiere politiche e giuridiche che rallentano la cooperazione internazionale tra le autorità giudiziarie e consentono alla criminalità organizzata di scegliere lo Stato più adatto alla realizzazione delle proprie attività illecite³⁰⁰.

Nondimeno, è emersa una ulteriore esigenza sempre più rilevante sulla scena internazionale: il contrasto al *cybercrime*, ossia la lotta a un crimine che in qualche modo è collegato ad elementi di carattere informatico. Tale fenomeno diventa ancora più difficile da contrastare dal momento in cui è possibile arrecare un danno a un bene giuridicamente protetto allocato in qualsiasi parte del globo terrestre pur essendo l'agente a molti chilometri di distanza. In tale contesto si contrappongono l'“anarchia di internet” e l'“anarchia del diritto”.

È proprio partendo da tale dato che bisognerebbe chiedersi se la cooperazione giudiziaria non sia essa stessa una esigenza ineludibile ed analizzare lo sviluppo funzionale di uno spazio penale europeo volto alla libertà, sicurezza e giustizia.

1.1. (Segue). *La “quinta libertà” e la cooperazione giudiziaria come esigenza*

Com'è noto, l'art. 26 TFUE specifica che il mercato interno all'Unione Europea «comporta uno spazio senza frontiere, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali». A causa di queste quattro libertà si è sviluppata, quale effetto collaterale, una quinta libertà “sgradita”³⁰¹: la libera circolazione dei criminali e del crimine.

Queste libertà comportano non solo effetti positivi e benefici in tutta l'area dell'Unione Europea, quali il libero commercio transfrontaliero e la velocità dei traffici, ma anche effetti particolarmente negativi da contrastare, come l'aumento dei fenomeni di criminalità transfrontaliera.

Da qui sorgono le esigenze alla base della cooperazione giudiziaria. Volendo schematizzare, è possibile dividerle in base alla loro eziologia in:

- esigenze a causa negativa;
- esigenze a causa positiva.

Nel primo gruppo sono ricomprese tutte le esigenze nate per combattere la criminalità transfrontaliera come, più in generale, la lotta ai *cross-border crimes*, il traffico di sostanze stupefacenti, il traffico di armi, la tratta di esseri umani, la pedopornografia, sfruttamento sessuale delle donne, i *cyber-crimes*, ma anche la lotta al terrorismo internazionale, alla corruzione, ai reati ambientali, alla criminalità organizzata e ai reati economici e societari, quali il riciclaggio e la contraffazione di mezzi di pagamento. Inoltre, a tale insieme appartiene la necessità di agevolare lo svolgimento di quei procedimenti penali che, pur non riguardando crimini transfrontalieri in senso stretto, richiedono in uno Stato terzo il compimento di atti procedurali per i quali difetta la giurisdizione.

³⁰⁰ In tal senso si veda M. PELLEGRINO, *Cooperazione giudiziaria penale nell'U.E.*, Padova, 2016, p. 14 ss.

³⁰¹ L'espressione “quinta libertà” è di J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R. E. KOSTORIS), cit., p. 346.

Al secondo gruppo appartengono, invece, tutte quelle esigenze relative alle garanzie come il rispetto dei diritti umani, delle libertà fondamentali e, più nello specifico, dei principi del giusto processo, dei diritti degli indagati e degli imputati, dei diritti della vittima, dei diritti dei detenuti, del diritto alla privacy, della libertà personale e della dignità umana³⁰².

Se è vero che le esigenze – *alias* i bisogni, le necessità – trovano un loro efficace strumento di soddisfazione nella cooperazione giudiziaria in materia penale, è vero anche che tale cooperazione giudiziaria diventa essa stessa esigenza.

Infatti, la cooperazione giudiziaria in quanto attività di collaborazione internazionale nella lotta contro il crimine compiuta dall'autorità giudiziaria di uno Stato nell'ambito di un procedimento pendente o già celebrato in uno Stato terzo³⁰³ rappresenta il solo strumento utilizzabile per garantire un'efficace risposta a quanto sinora illustrato, assurgendo essa stessa a metodo indispensabile, in quanto esclusivo mezzo efficiente, e quindi necessario, nella lotta alla criminalità internazionale.

Ad oggi, esso rappresenta l'unico sistema capace di evitare una totale cessione di sovranità degli Stati, i quali, così facendo, scongiurano il pericolo che si gridi nei loro confronti "il re è nudo"³⁰⁴, poiché non rivelano una propria debolezza, anzi, dimostrano di non esser disarmati di fronte alle nuove sfide, contrapponendo alla libertà di circolazione dei criminali e del crimine una "quinta libertà di circolazione" positiva, quella, cioè, propria dei provvedimenti giurisdizionali nello spazio giudiziario europeo, concorrendo alla tutela degli interessi dell'Unione e al conseguimento dei suoi obiettivi³⁰⁵.

2. La disciplina della cooperazione giudiziaria in materia penale nell'Unione europea

Per garantire le quattro libertà fondamentali nell'Unione europea, non si può effettivamente prescindere da un sistema garante di elevati *standard* di libertà, sicurezza e giustizia perseguibili abbandonando gli ormai vecchi ed arrugginiti strumenti basati sui principi di sovranità e territorialità e sviluppando tecniche di cooperazione più moderne ed efficienti nella *single legal area*³⁰⁶.

In ambito europeo, la disciplina relativa alla cooperazione giudiziaria in materia penale è contenuta nella Parte seconda, Titolo V, al Capo IV del TFUE. Il Titolo V è relativo allo spazio di libertà, sicurezza e giustizia³⁰⁷, cioè un'area realizzata dall'Unione,

³⁰² Si tratta di un elenco aperto, non esaustivo né tantomeno tassativo. Ciò che interessa rilevare è come la cooperazione giudiziaria in materia penale si sia sviluppata seguendo queste due direttrici che hanno il merito da una parte di garantire la sicurezza sull'intero territorio dell'Unione Europea, dall'altra di ampliare le garanzie già riconosciute dai singoli Stati membri.

³⁰³ M. PELLEGRINO, *Cooperazione giudiziaria nell'U.E. Dalle origini alla Procura europea*, cit., p.13.

³⁰⁴ La frase è tratta dalla famosissima fiaba danese "I vestiti nuovi dell'imperatore" scritta da Hans Christian Andersen e pubblicata per la prima volta nel 1837 nel volume "Fiabe, raccontate per i bambini".

³⁰⁵ Cfr., S. MONTALDO, *I limiti della cooperazione in materia penale nell'Unione europea*, cit., p. 19 ss.

³⁰⁶ Sul punto, G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all'ordine di indagine*, cit., p. 8.

³⁰⁷ Lo spazio di libertà, sicurezza e giustizia è uno dei principali obiettivi fissati dall'art. 3 TUE. Ed invero, l'art. 3, par. 2, TUE, recita: «l'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persona insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione

della criminalità e la lotta contro quest'ultima». Si tratta, quindi, di un effetto auspicato dell'azione delle istituzioni dell'Unione europea, insieme con la promozione della pace, dei suoi valori e del benessere dei popoli. Si veda, in dottrina, A. DI STASI, *Tutela multilevel dei diritti fondamentali e costruzione dello spazio europeo di giustizia*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale del titolo VI della Carta* (a cura di A. DI STASI), Napoli, 2019, p. 11 ss. Secondo l'A., la strutturazione dello spazio «intorno ad un trinomio di “principi-valori” quali libertà, sicurezza e giustizia – che assurgono a elementi costitutivi di pari valenza ma, per loro natura, anche in potenziale contrapposizione – rende ineludibile un'attività di costante bilanciamento tra di essi (ad opera di un complesso di attori e, *inter alia*, i giudici) il tutto nella direzione della piena garanzia dei diritti fondamentali che, unitamente al rispetto dei diversi ordinamenti giuridici e delle differenti tradizioni giuridiche degli Stati membri, rappresentano fattori necessari per la realizzazione di uno spazio europeo comune se non unitario. La non facile individuazione di un punto di equilibrio tra libertà, sicurezza e giustizia con riferimento specifico alla creazione dello *spazio europeo di giustizia*, quale segmento del più ampio spazio giuridico e giudiziario europeo, non può prescindere – soprattutto in ambito penale – da una “costante tensione verso il contemperamento al più alto grado delle esigenze securitarie con quelle della assoluta garanzia offerta ai diritti fondamentali”». Più in generale, v. anche, M. FLETCHER, E. HERLIN-KARNELL, C. MATERA (eds.), *The European Union as an Area of Freedom, Security and Justice*, London e New York, 2016; C. CHEVALLIER-GOVERS, *L'Espace de liberté, de sécurité et de justice (ESLJ)*, cit., p. 114 ss.; N. NAVARRO BATISTA, *The development and consolidation of the Area of Freedom, Security and Justice*, cit., p. 389 ss.; M.J. BORGERS, *Functions and aims of harmonisation after the Lisbon Treaty: a European Perspective*, in AA.VV., *The future of police and judicial cooperation in the European Union* (C. FIJNAUT, J. OUWERKERK eds.), Leiden, 2010, p. 347 ss.; M. CHIAVARIO, *Giustizia europea e processo penale: nuovi scenari e nuovi problemi*, in AA.VV., *Processo penale e giustizia europea. Omaggio a Giovanni Conso* (a cura di U. DRAETTA, N. PARISI), Milano, 2010, p. 229 ss.; F. CLEMENTI, *Lo spazio di libertà, sicurezza e giustizia*, in AA.VV., *Le nuove istituzioni europee: commento al Trattato di Lisbona* (a cura di D. RINOLDI), Bologna, 2010, p. 201 ss.; H. LABAYLE, *La nouvelle architecture de l'espace de liberté, de sécurité et de justice*, in C. KADDOUS, M. DONY (eds.), *D'Amsterdam à Lisbonne*, Bruxelles, 2010, p. 3 ss.; J. MONAR (ed.), *The institutional dimension of the European Union's area of freedom, security and justice*, Bruxelles, 2010; D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia*, Napoli, 2010; C. CHEVALLIER-GOVERS, *Le traité de Lisbonne et la différenciation dans l'espace de liberté, de sécurité et de justice*, in E. BROSSET, C. CHEVALLIER-GOVERS, V. EDJAHARIAN, *Le traité de Lisbonne: déconstitutionnalisation ou reconfiguration de l'Union européenne?*, Bruxelles, 2009, p. 263 ss.; F. JAULT-SESEKE, J. LELIEUR, C. PIGACHE (eds.), *L'espace judiciaire européen civil et pénal: regards croisés: actes du 25e colloque des Instituts d'études judiciaires, 20-21 mars 2009 à l'Université de Rouen*, Paris, 2009; E. SHARPSTON, *The future of the area of freedom, security and justice*, in M. DOUGAN, S. CURRIE (eds.), *50 years of the European treaties*, Oxford, 2009, p. 219 ss.; E. BARBE, G. RENAUDINEAU, *L'espace de liberté, de sécurité et de justice*, in J. ZILLER, *L'Union européenne: édition traité de Lisbonne*, Paris, 2008, p. 63 ss.; R. CAFARI PANICO, *Lo spazio di libertà, sicurezza e giustizia nel Trattato di riforma e nel Trattato costituzionale*, in AA.VV., *Dalla Costituzione europea al Trattato di Lisbona* (a cura di M.C. BARUFFI) Padova, 2008, p. 81 ss.; M.G.W. DEN BOER, *A diagnosis of the area of freedom, security and justice: remedies and reforms in the domains of immigration, terrorism and security*, in S. BLOCKMANS, S. PRECHAL (eds.), *Reconciling the deepening and widening of the European Union*, The Hague, 2007, p. 13 ss.; U. DRAETTA, N. PARISI, D. RINOLDI (a cura di), *Lo spazio di libertà, sicurezza e giustizia dell'Unione europea: principi fondamentali e tutela dei diritti*, Napoli, 2007; T. KOSTAKOPOULOU, *The area of freedom, security and justice and the European Union's constitutional dialogue*, in C. BARNARD (ed.), *The fundamentals of EU law revisited*, USA, 2007, p. 153 ss.; L. SALAZAR, *La costruzione di uno spazio penale comune europeo*, in AA.VV., *Lezioni di diritto penale europeo* (a cura di G. GRASSO, R. SICURELLA), cit., p. 395 ss.; F. LONGO, *L'area di libertà, sicurezza e giustizia nella prospettiva politologica*, in AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007, p. 69 ss.; R.L. HOLZHACKER, P. LUIF, *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation After the Lisbon Treaty*, New York, 2014; A.H. GIBBS, *Constitutional Life and Europe's Area of Freedom Security and Justice*, England-USA, 2013; U. GUERINI, *Il terzo pilastro dell'Unione europea: uno spazio di libertà, sicurezza e giustizia*, in AA.VV., *Il diritto penale dell'Unione europea. La normativa, la dottrina, la giurisprudenza europea in materia penale e la cooperazione giudiziaria*, Torino, 2008, p. 75 ss.; E. GUILD, F. GEYER, *Security Versus Justice? Police and Judicial Cooperation in the European Union*, Great Britain, 2013; S. MANACORDA, *La consolidation de l'espace de liberté, de sécurité et de justice: vers une “mise à*

in cui ai sensi dell'art. 67 TFUE è garantito che: non vi siano controlli sulle persone alle frontiere; si sviluppi una politica comune in materia di asilo, immigrazione e controllo delle frontiere esterne, fondata sulla solidarietà tra gli Stati membri ed equa nei confronti dei cittadini dei Paesi terzi; vi sia un elevato livello di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra le forze di polizia, autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali; sia facilitato l'accesso alla giustizia, in particolare attraverso il principio di riconoscimento reciproco delle decisioni giudiziarie ed extragiudiziali in materia penale.

Il Capo IV rappresenta un contenitore ove sono racchiuse le norme relative alla cooperazione giudiziaria in materia penale. Gli art. 82 e ss., TFUE, basandosi sulle Conclusioni del Consiglio europeo di Tampere, disciplinano la materia in maniera specifica, articolandola su un "doppio binario" e prevedendo due strumenti: da una parte vi è l'attuazione del principio del riconoscimento reciproco delle sentenze e delle decisioni giudiziarie, dall'altra si prevede il ravvicinamento delle disposizioni legislative e regolamentari degli Stati Membri.

Se si presta bene attenzione al "doppio binario", si nota come la cooperazione giudiziaria sia "fondata" sul principio del reciproco riconoscimento delle decisioni giudiziarie ed "include" il ravvicinamento normativo³⁰⁸. È quindi importante sottolineare – e sarà oggetto di trattazione specifica nel presente lavoro – come il principio del mutuo riconoscimento, insieme con il ravvicinamento delle legislazioni, sia fondamentale per l'instaurazione e il rafforzamento di una reciproca fiducia tra gli Stati membri dell'Unione³⁰⁹.

L'art. 82 TFUE³¹⁰ divide la cooperazione giudiziaria in materia penale in due gruppi di materie in base alla tipologia di atti utilizzabili: da una parte, il paragrafo 1 individua

l'écart” du rapprochement pénal, in *Revue de science criminelle et de droit penal comparé*, 4, 2007, p. 899 ss. Per un interessante bilancio a vent'anni dal Consiglio di Tampere, attraverso un *focus* su quattro ambiti (dialogo tra le corti, cooperazione giudiziaria in materia civile, cooperazione giudiziaria in materia penale, flussi migratori), A. DI STASI, L.S. ROSSI (a cura di), *Lo spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, Napoli, 2020.

³⁰⁸ Cfr. A. DI STASI, *Spazio europeo di libertà, sicurezza e giustizia e cooperazione giudiziaria in materia penale: il rispetto dei diritti fondamentali e della diversità tra ordinamenti nazionali e tradizioni giuridiche*, in «*Spazio europeo di giustizia*» e *procedimento penale italiano*, (a cura di L. KALB), cit., p. 20.

³⁰⁹ Sul rapporto tra gli Stati membri e sul rafforzamento della reciproca fiducia si veda anche B. NASCIMBENE, *Lo spazio di libertà, sicurezza e giustizia a due anni dall'entrata in vigore del Trattato di Lisbona*, in *Dritto, immigrazione e cittadinanza*, 4, 2011, p. 13 ss.; D. FLORE, *La notion de confiance mutuelle: l'“alpha” ou l'“omega” d'une justice pénale européen*, in AA.VV., *La confiance mutuelle dans l'espace pénal européen* (a cura di G. DE KERCHOVE, A. WEYEMBERGH), Bruxelles, 2005, p. 17 ss.; R. ADAM, *La cooperazione in materia di giustizia e affari interni tra comunitarizzazione e metodo intergovernativo*, in *DUE*, 2/3, 1998, p. 481 ss.; N. PARISI, *Tecniche di costruzione di uno spazio penale europeo. In tema di riconoscimento reciproco delle decisioni giudiziarie e di armonizzazione delle garanzie procedurali*, in *I quaderni europei*, 2012, p. 5 ss.

³¹⁰ Sul tema la dottrina è molto ampia. Si segnalano, *ex multis*, C. AMALFITANO, *L'azione dell'Unione Europea per la tutela delle vittime di reato*, in *Il Diritto dell'Unione europea*, 2011, p. 643 ss.; ID., *Conflitti di giurisdizione e riconoscimento delle decisioni penali nell'Unione Europea*, Milano, 2006; A. BERNARDI, *La competenza penale accessoria dell'Unione europea: problemi e prospettive*, in *Dir. pen. cont.*, 1, 2012, p. 43 ss.; M. CHAVES, *EU's Harmonization of National Criminal Law: Between Punitiveness and Moderation*, in *European public law*, 3, 2015, p. 57 ss.; M. CONDINANZI, *Fonti del “terzo pilastro” dell'Unione europea e ruolo della Corte costituzionale*, in *Diritto dell'Unione Europea*, 2007, p. 513 ss.; R. MASTROIANNI, *Diritto dell'Unione europea e processo penale: un'introduzione*, in AA.VV., *L'integrazione europea attraverso il diritto processuale penale* (a cura di R. MASTROIANNI, D. SAVY),

tutti i settori passibili di uniformazione giuridica. In tal caso, il Parlamento europeo e il Consiglio, con procedura ordinaria, adottano misure per: la definizione di norme e procedure volte ad assicurare il riconoscimento nell'Unione Europea "di qualsiasi tipo di sentenza e decisione giudiziaria" (lett. a); la prevenzione e risoluzione dei conflitti di giurisdizione tra gli Stati membri (lett. b); il sostegno della formazione dei magistrati e degli operatori giudiziari (lett. c); la facilitazione della cooperazione tra le autorità giudiziarie e le autorità omologhe degli Stati membri rispetto all'azione penale e all'esecuzione delle decisioni (lett. d)³¹¹. Dall'altra al paragrafo 2 si elencano tassativamente gli ambiti materiali del diritto processuale e sostanziale penale passibili solo di un ravvicinamento normativo e regolamentare tra gli Stati membri, tra cui si evidenziano l'ammissibilità reciproca delle prove tra gli Stati membri (lett. a), i diritti della persona nella procedura penale (lett. b), i diritti delle vittime nella criminalità (lett. c)³¹². Una clausola aperta, infine, consente l'individuazione di altri settori ove è possibile un ravvicinamento, previa individuazione di essi in via preliminare da parte del Consiglio con una decisione. La decisione è adottata con approvazione del Parlamento e deliberazione all'unanimità del Consiglio.

Il ravvicinamento delle legislazioni – sotto il profilo tanto processuale quanto sostanziale – va perseguito soltanto se necessario al rafforzamento della cooperazione giudiziaria e per facilitare il riconoscimento reciproco delle sentenze e delle decisioni giudiziarie.

Ad una prima lettura, il ravvicinamento delle legislazioni sembrerebbe avere solo una funzione servente rispetto alla libera circolazione delle decisioni penali nel territorio europeo degli Stati membri. In realtà, come attenta dottrina fa notare, la funzione precipua è quella di evitare i fenomeni di *forum shopping*, ma soprattutto garantire una certa parità di trattamenti tra i cittadini dei diversi Stati membri, impedendo le discriminazioni relative ai comportamenti punibili e alle sanzioni applicabili al fine di creare un sentimento comune di giustizia all'interno dello spazio europeo di libertà, sicurezza e giustizia³¹³.

Per attuare tutto ciò, è stato innescato un processo evolutivo irreversibile di trasformazione della tradizionale cooperazione tra Stati in una *cooperazione tra giurisdizioni*, che elimina il rapporto tra le amministrazioni a favore di quello tra sole giurisdizioni, e che tende sempre di più verso qualcosa che può definirsi giustizia transnazionale o addirittura, come sottolineato da parte della dottrina, una progressiva "integrazione tra le giurisdizioni"³¹⁴.

Napoli, 2013, p. 3 ss.; J. ÖBERG, *The legal basis for Eu criminal law harmonisation. A question of federalism?*, in *European law review*, 3, 2018, p. 366 ss.; T. RAFARACI, *La cooperazione di polizia e giudiziaria in materia penale nell'Unione Europea dopo il trattato di Lisbona*, Milano, 2011; G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice Review*, 1, 2019, p. 84 ss.; L. SALAZAR, sub art. 82 TFUE, in AA.VV., *Codice dell'Unione europea operativo* (diretto da C. CURTI GIALDINO), Napoli, 2012, p. 896 ss.

³¹¹ Si veda E. PISTOIA, *Cooperazione penale nei rapporti tra diritto dell'Unione Europea e diritto statale*, (a cura di E. PISTOIA), Napoli, 2008, p. 221 ss.

³¹² C. AMALFITANO, sub Art. 82 TFUE, in AA.VV., *Trattati dell'Unione Europea* (a cura di A. TIZZANO), II ediz., Milano, 2014, p. 866 ss.

³¹³ C. AMALFITANO, sub Art. 82 TFUE, in AA.VV., *Trattati dell'Unione Europea* (a cura di A. TIZZANO), cit., p. 874.

³¹⁴ M. PISANI, *Criminalità organizzata e cooperazione internazionale*, in *Riv. it. dir. proc. pen.*, 3, 1998, 703 ss.; E. SELVAGGI, *Criminalità transnazionale e cooperazione giudiziaria internazionale*, in AA.VV., *Criminalità transnazionale fra esperienze europee e risposte penali globali*. Atti del III Convegno

Da ciò, nasce la consapevolezza dell'Unione Europea del fatto che così come si muovono liberamente le persone, anche le decisioni giudiziarie devono poter circolare senza alcun ostacolo. La cooperazione giudiziaria in materia penale non deve in alcun modo essere d'intralcio alla libera circolazione delle persone, dei servizi, delle merci e dei capitali, così come da sempre evidenziato dalla stessa Corte di Giustizia dell'Unione Europea³¹⁵.

L'art. 82, par. 2, TFUE sottolinea inoltre che le eventuali norme minime di sostegno al riconoscimento reciproco delle decisioni giudiziarie e la cooperazione giudiziaria in materia penale debbano tener conto "delle differenze tra le tradizioni giuridiche e gli ordinamenti giuridici degli Stati membri".

Ciò perché l'Unione europea ha piena consapevolezza delle caratteristiche molto diverse possedute dagli Stati membri, in quanto dotati di sistemi giudiziari eterogenei e, di conseguenza, incapaci di trattare in maniera uguale o addirittura simile le singole questioni processuali senza un'attività di integrazione. Per perfezionare lo spazio europeo di libertà, sicurezza e giustizia bisogna tener conto di tale dato incontrovertibile, nonché delle disposizioni delle diverse costituzioni di cui i singoli Stati sono dotati.

Ne deriva che l'unico modo per attuare una cooperazione giudiziaria in materia penale efficace ed efficiente sia quella di sviluppare una cultura giudiziaria europea attraverso il rafforzamento della reciproca fiducia e di attuare, per quanto possibile, una convergenza di norme sostanziali e processuali, nonché di istituti e categorie giuridiche comuni³¹⁶.

Grazie allo strumento dell'assistenza giudiziaria in materia penale gli Stati possono prestarsi reciproca assistenza nella lotta contro la criminalità internazionale³¹⁷. In particolare, l'assistenza giudiziaria *in rem* ha ad oggetto lo svolgimento di una attività istruttoria diretta ad acquisire le prove relative ad un certo reato e può consistere: nell'audizione di testimoni e imputati, nel sequestro a titolo conservativo e nella consegna di prove, documenti ed altri beni pertinenti al reato, nella perquisizione domiciliare, nella notificazione di sentenze e di altri atti giudiziari che non possono essere eseguite nel territorio dello Stato richiedente.

3. (Segue). La cooperazione "verticale" e la cooperazione "orizzontale"

Si è appurato come la cooperazione giudiziaria sia, molto semplicemente, uno strumento di lotta alla criminalità transnazionale consistente nell'attività di collaborazione tra gli Stati. Più in particolare, la dottrina, nel dare una definizione di "cooperazione giudiziaria europea" si divide in chi adotta una definizione soggettiva

Internazionale promosso dal Centro Studi Giuridici "Francesco Carrara". Lucca, 24-25 maggio 2002, Milano, 2005, p. 415 ss.

³¹⁵ Cfr., per tutte, Corte di giustizia, sentenza 11 febbraio 2003, cause riunite C-187/01 e C-385/01, *Gözütok e Brügge*, I-1345, punti 36-38; Corte di giustizia, sentenza 28 giugno 2012, causa C-192/12 PPU, *West*, punto 73. Invece, in dottrina, si veda S. PEERS, *Mutual recognition and criminal law in the European Union: has the council got it wrong*, in *Common Market Law Review*, 1, 2004, p. 5 ss.

³¹⁶ Si veda sul punto A. GAMBARO, R. SACCO, *Sistemi giuridici comparati*, Torino, 2009, p. 305.

³¹⁷ Ad esempio, il giudice che deve svolgere indagini nel territorio di uno Stato estero può chiedere alle autorità giudiziarie di quello Stato di eseguirle e di trasmettere i risultati al Paese in cui si celebra il processo. La materia dell'assistenza giudiziaria è disciplinata, nell'ordinamento italiano, dalla Costituzione (art. 10); dalla legge (Libro XI, titolo III, artt. 723 ss. c.p.p.; artt. 201-206 norme di attuazione c.p.p.); dalle Convenzioni internazionali e dalle norme di Diritto internazionale generale, nonché dal diritto dell'Unione europea che, in base al disposto dell'art. 696 c.p.p., laddove esistenti prevalgono sulle norme di legge ordinaria, in applicazione del principio di prevalenza, sussidiarietà e di residualità.

guardando alla struttura e chi una oggettiva, guardando alla funzione. Secondo il punto di vista soggettivo per cooperazione giudiziaria europea si indica il complesso «movimento europeistico che, muovendo dalla collaborazione interstatuale sul mero piano dell'unione internazionale, giunge a costituire veri e propri organismi la cui attività incide, in modo diretto, sulla struttura dell'Unione dei Paesi europei»³¹⁸; per chi invece abbraccia la definizione oggettiva e guarda alla funzione, la cooperazione giudiziaria a livello europeo consisterebbe nell'agevolare la cooperazione tra gli operatori della giustizia come giudici, pubblici ministeri e avvocati difensori e i loro omologhi in altri Stati membri, migliorare il riconoscimento reciproco delle decisioni giudiziarie in materia penale tra gli Stati membri, provvedere, se necessario, al ravvicinamento del diritto sostanziale e procedurale, controllare l'applicazione della normativa adottata e tenere conto degli aspetti attinenti alle relazioni esterne della giustizia penale (relazioni con Paesi non appartenenti all'UE)³¹⁹.

Nel villaggio globale, ed in particolare in quello europeo, non si può più fare a meno di istituzioni giudiziarie e di organismi di polizia comuni, che rendano effettiva e facciano avvertire la forza coercitiva della realtà politica rappresentata dall'Unione Europea.

Nasce così una cooperazione multilivello in ragione degli attori che si affacciano ad operare e del rapporto che si instaura tra loro. Si sviluppa, allora, da una parte la cooperazione giudiziaria verticale e dall'altra la cooperazione giudiziaria orizzontale³²⁰.

Caratteristica della cooperazione giudiziaria verticale è prevedere l'intervento di organismi sovranazionali la cui azione procede dall'alto verso il basso, ossia dal livello europeo al livello nazionale. Alla cooperazione giudiziaria verticale si contrappone la cooperazione giudiziaria orizzontale, la quale si realizza quando più Stati cooperano tra di loro.

Gli organismi sovranazionali facenti parte della cooperazione giudiziaria verticale, in realtà, non esercitano dei poteri autoritativi nei confronti degli organi investigativi degli Stati membri, ma più semplicemente hanno lo scopo di agevolare e supportare le attività investigative quando l'oggetto di indagine assume delle caratteristiche di transnazionalità. Protagonisti diventano Eurojust, Olaf, Europol ed EPPO. Tali strutture alimentano il rapporto di reciproca fiducia tra le autorità giudiziarie dei Paesi membri attraverso la creazione di reti che creano uno spazio giudiziario comune ed assumono fondamentali funzioni sostanzialmente assimilabili a quelle esercitate dagli organi investigativi degli Stati membri, nonostante non vi sia un vero e proprio sistema processuale penale europeo. L'obiettivo è quello di attuare il principio della territorialità europea e il principio della libera circolazione delle decisioni giudiziarie.

Attualmente, l'Olaf svolge indagini amministrative e, in tale contesto, raccoglie ed elabora le *notitiae criminis* relative ai reati contro gli interessi finanziari dell'Unione

³¹⁸ La definizione è di A. IANNUZZI, *La cooperazione tra le autorità di polizia*, in «Spazio europeo di giustizia» e *procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), cit., p.147.

³¹⁹ Si veda, *ex multis*, M. FIDELBO, *La cooperazione rafforzata come modalità d'istituzione della procura europea*, in *Riv. dir. pen. cont.*, 3, 2016, p. 92 ss.; C. AMALFITANO, *Spazio giudiziario europeo e libera circolazione delle decisioni penali*, in *Studi sull'integrazione europea*, 1, 2009, pp.73-120; N. PARISI, *Riconoscimento reciproco delle decisioni giudiziarie penali, confiance mutuelle e armonizzazione delle garanzie procedurali negli Stati membri dell'Unione europea*, in AA.VV., *Scritti in onore di Ugo Draetta* (a cura di N. PARISI, M. FUMAGALLI MERAVIGLIA, D. RINOLDI, A. SANTINI), Napoli, 2011, p. 503 ss.

³²⁰ Su questa distinzione, AA.VV., *Manuale di procedura penale* (a cura di R.E. KOSTORIS), cit., *passim*.

Europea, che trasmette alle autorità nazionali competenti dei singoli Stati membri per l'accertamento e il giudizio.

Europol, invece, offre attività di assistenza alle autorità competenti degli Stati membri raccogliendo dati e promuovendo lo scambio di informazioni al fine di contrastare le gravi forme di criminalità transnazionale.

Infine, Eurojust ha il compito fondamentale di incentivare la cooperazione giudiziaria in materia penale, migliorare il coordinamento delle indagini, dei procedimenti e lo scambio di informazioni tra le autorità competenti degli Stati membri in ipotesi di forme gravi di criminalità transnazionale, in particolare la criminalità organizzata. Inoltre, ha anche la facoltà di fornire assistenza nelle indagini e nei procedimenti che coinvolgono uno Stato membro ed uno Stato non membro, qualora sia stato concluso un accordo di cooperazione tra Eurojust e lo Stato non membro ovvero vi sia un interesse di carattere essenziale nell'offerta di tale assistenza³²¹.

Purtroppo, Eurojust, Europol e Olaf ad oggi, nonostante i grandi sforzi profusi per la causa, pur ottenendo ottimi risultati, appaiono ancora poco maturi per affrontare in maniera efficiente le nuove sfide poste dalla criminalità organizzata e dal terrorismo internazionale. Questo perché il carattere di "verticalità" che connota le diverse tipologie dei moduli di collaborazione sviluppati dalle tre grandi agenzie nel rapporto con le autorità dei diversi Stati membri non implica affatto l'esercizio di poteri autoritativi nei confronti degli organi investigativi nazionali, perché esse, allo stato, sono chiamate solo ad agevolare e supportare quando l'indagine assuma un rilievo transnazionale³²². D'altro canto, è vicina alla piena operatività una nuova istituzione: il pubblico ministero europeo, realizzata a partire da Eurojust, come dispone l'art. 86 TFUE.

Infatti, il 5 ottobre 2017 il Parlamento europeo ha dato il via libera alla creazione dell'*European Public Prosecutor Office* (Eppo)³²³, un ufficio giudiziario centrale contro la criminalità finanziaria nell'Ue³²⁴. La Procura europea – organismo indipendente – coordina le indagini nazionali sulle frodi a livello comunitario, ha legittimazione esclusiva, e deve perseguire penalmente gli abusi. Obiettivo è quello di garantire una

³²¹ Per un importante approfondimento, v. L. PALMIERI, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, cit., p. 49 ss. Secondo l'A., il nuovo regolamento «ha apportato modifiche sostanziali alle disposizioni contenute nella precedente Decisione istitutiva per quanto concerne i poteri dei membri nazionali, ridisegnando la struttura amministrativa e di gestione, al fine di sviluppare tutto il suo potenziale nella lotta contro le forme gravi di criminalità transfrontaliera. In quest'ottica, il regolamento ha implementato le *funzioni operative di Eurojust* – riducendo, così, il carico di lavoro "amministrativo" in precedenza attribuito ai membri nazionali – ed ha realizzato una proficua *governance* dell'organismo attraverso l'istituzione del Comitato esecutivo (che assisterà il Collegio nelle funzioni di gestione) e del Direttore amministrativo». Sia consentito il rinvio anche ad A. GAUDIERI, *La nuova Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust)*, in *Osservatorio SLSG*, novembre 2018, consultabile al link: <https://www.unisa.it/uploads/14394/audieri.nov.2018.pdf>.

³²² G. DE AMICIS, *Organismi europei di cooperazione e coordinamento investigativo*, relazione tenuta al XXX Convegno nazionale "Investigazioni e prove difensive", organizzato dall'Associazione tra gli Studiosi del Processo Penale "G. D. Pisapia", in Roma, il 20-21 ottobre 2016.

³²³ Il Regolamento (UE) 2017/1939 del Consiglio relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea (EPPO) è stata pubblicata in GUUE, L 283 del 31 ottobre 2017. Per un approfondimento, L. KALB, *Questioni problematiche in tema di Procura europea*, in AA.VV., *Lo spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. DI STASI, L.S. ROSSI), Napoli, 2020, p. 291 ss.

³²⁴ Solo 20 Stati hanno raggiunto un accordo sull'istituzione della Procura europea: Austria, Belgio, Bulgaria, Cipro, Croazia, Estonia, Finlandia, Francia, Germania, Grecia, Italia, Lettonia, Lituania, Lussemburgo, Portogallo, Repubblica Ceca, Romania, Slovacchia, Spagna e Slovenia. Gli Stati che non hanno aderito potranno comunque farlo in qualsiasi momento, anche dopo l'adozione del regolamento.

maggiore efficacia dell'azione penale e il recupero delle somme oggetto di frode. I procuratori operano come un organismo unico con procedure semplificate, e svolgono le indagini su tutto il territorio degli Stati membri, scambiandosi in maniera rapida le informazioni utili in modo da assicurare il coordinamento delle indagini, la confisca e, quando indispensabile, chiedendo l'arresto dei sospetti nell'ambito di una strategia europea comune in materia di indagini e di azioni penali.

La Procura europea ha una struttura collegiale costruita su due livelli:

- a livello centrale vi è il “procuratore europeo” che avrà la responsabilità generale dell'ufficio ed è assistito da quattro sostituti procuratori. Compiti specifici sono il monitoraggio, la direzione e il controllo di tutte le indagini e le azioni penali intraprese dai procuratori delegati europei, al fine di garantire la coerenza delle indagini in tutta l'Unione. Può revocare i procuratori europei delegati se non rispondono più ai requisiti necessari per l'esercizio delle loro funzioni;
- il livello periferico, invece, è costituito dai “procuratori delegati europei”, attivi nei singoli Stati membri, che hanno il compito di svolgere le indagini ed esercitare l'azione penale, seguendo il Regolamento della Procura europea e la legislazione dello Stato membro.

Per quanto riguarda la cooperazione orizzontale, si distinguono gli strumenti della cooperazione di polizia dagli strumenti di cooperazione giudiziaria.

Appartengono alla categoria degli strumenti della cooperazione di polizia tutta una serie di modalità operative previste dalla Convenzione applicativa dell'Accordo di Schengen (CAAS) tra cui l'osservazione transfrontaliera, l'inseguimento transfrontaliero nonché il distacco di funzionari di collegamento e il sistema di informazione Schengen (S.I.S. e S.I.S. II).

Fanno parte, invece, degli strumenti di cooperazione giudiziaria il magistrato di collegamento, la Rete giudiziaria europea, la trasmissione spontanea di informazioni e le squadre investigative comuni. Anche il mandato di arresto europeo e l'ordine europeo di indagine penale possono esser ricompresi tra gli strumenti di cooperazione giudiziaria e di polizia orizzontale aventi il fine di rafforzare l'assistenza giudiziaria tra gli Stati membri, siccome tali istituti prevedono il diretto contatto tra autorità giudiziarie dei diversi Paesi dell'Unione europea.

4. Le nuove sfide e gli sviluppi della cooperazione giudiziaria in materia penale nell'Unione europea

Come si è osservato, la nozione di “spazio europeo di libertà, sicurezza e giustizia” è un concetto innovativo ed originale in quanto consente agli Stati di abbandonare la classica accezione di sovranità nazionale per approdare alla nozione di “sovranità condivisa”, ove l'azione coercitiva penale diventa di respiro europeo e non solo interno ad un singolo Stato.

Il concetto, seppur astratto e dinamico perché opera tra Stati con caratteristiche ed identità differenti uniti da principi comuni in un contesto unico ed unitario, rimanda a quel duro lavoro ancora in atto di ricerca di una unità normativa rispettosa delle diversità

e delle complessità degli ordinamenti³²⁵. È necessario, quindi, comprendere qual è stato il lungo e tortuoso percorso compiuto per arrivare alla cooperazione giudiziaria in materia penale nell'area dell'Unione Europea e quali sono i principi di riferimento attuali.

I Trattati istitutivi delle Comunità europee contenevano già l'embrione della futura cooperazione giudiziaria tracciata nei trattati successivi e che potrebbe evolvere in un sistema penale europeo compiuto. Con il Trattato di Maastricht maturò il concetto di "cooperazione giudiziaria" nel c.d. terzo settore e con il Trattato di Amsterdam nacque il concetto di "spazio giudiziario"³²⁶. La gestazione fu effettivamente lunga e travagliata a causa delle continue emergenze sorte: criminalità transnazionale, criminalità finanziaria e terrorismo.

Dopo il Consiglio di Tampere del 1999³²⁷ si è sviluppata una normativa sul tema tanto articolata e sovrabbondante quanto probabilmente confusionale a causa di esigenze che sorgevano l'una dopo l'altra in tempi ridottissimi. Accanto, sono nate tutta una serie di strutture sovranazionali di coordinamento investigativo³²⁸ con competenze tra loro spesso sovrapponibili.

La nascita della cooperazione giudiziaria in materia penale ruota intorno ad attività di contrasto di condotte di frode del bilancio comunitario o di corruzione ovvero a casi di reati collegati comunque all'economia e alla finanza³²⁹. Solo successivamente si sviluppa

³²⁵ Si veda la Presentazione del già Presidente di Eurojust José Luís Lopes da Mota in E. APRILE, F. SPIEZIA, *Cooperazione giudiziaria penale nell'Unione Europea prima e dopo il Trattato di Lisbona*, Milano, 2009.

³²⁶ L'espressione è coniata dal già Presidente francese Valéry Giscard d'Estaing, divenuto poi Presidente della Convenzione europea da cui nacque il progetto di Costituzione per l'Europa, nella seconda metà degli anni '70. Fu lui, infatti, il primo ad utilizzare la locuzione "*espace judiciaire européen*" per indicare l'area geografica dove trovano applicazione uniformemente i provvedimenti giudiziari emanati da uno Stato al di fuori dei propri confini territoriali.

³²⁷ Sul Consiglio di Tampere, A. DI STASI, *Il perfezionamento dello spazio europeo di libertà, sicurezza e giustizia: avanzamenti e criticità*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia* (a cura di A. DI STASI), cit., p. 117 ss.

³²⁸ Europol, Olaf, Eurojust, Rete giudiziaria europea. Il rischio era non solo quello di non garantire i diritti fondamentali dell'Unione Europea, ma anche quello di avere organismi che, avendo competenze sovrapponibili o concorrenti, fossero tra di loro di intralcio nelle attività svolte in assenza di un effettivo coordinamento, e di un'autorità giudiziaria preposta al controllo degli organi d'indagine europei.

³²⁹ Un esempio di tutto ciò può essere ravvisato nella legittimazione della Procura europea. Il Procuratore Europeo è legittimato per i reati che ledono interessi finanziari dell'Unione, i cc.dd. reati PIF, e per altri reati collegati a questi e basati sui medesimi fatti, purché i reati di tipo finanziario siano prevalenti. Il riferimento è all'art. 86, par. 2, TFUE il quale recita: «La Procura europea è competente per individuare, perseguire e rinviare a giudizio, eventualmente in collegamento con Europol, gli autori di reati che ledono gli interessi finanziari dell'Unione, quali definiti dal regolamento previsto nel paragrafo 1, e i loro complici. Essa esercita l'azione penale per tali reati dinanzi agli organi giurisdizionali competenti degli Stati membri». Il Regolamento 2017/1939/UE del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»), in GUUE 31 ottobre 2017, L 283, detta una serie di previsioni relative alla legittimazione dell'ufficio inquirente europeo. Per un approfondimento, L. KALB, *Questioni problematiche in tema di Procura europea*, in AA.VV., *Lo spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. DI STASI, L.S. ROSSI), cit., p. 297 ss.; ID., *Gli insegnamenti di un Maestro per lo studio delle nuove sfide: l'istituzione della Procura europea*, in AA.VV., *Liber amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), Napoli, 2020, p. 1121 ss.; L. PALMIERI, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, Milano, 2019, p. 88 ss.

Sia il TFUE sia il regolamento, come l'intera produzione normativa, utilizzano il termine competenza. In realtà, potrebbe sembrare più opportuno utilizzare la parola legittimazione. Questo perché la competenza è istituto del processo e non del procedimento. Essa rimanda a criteri prestabiliti dalla legge e immutabili in ragione del rispetto dello *status* di giudice naturale precostituito per legge, ossia per

anche in altri campi come traffico di esseri umani, stupefacenti, pedofilia, criminalità organizzata ed infine, con specifico riferimento ai temi oggetto di questo lavoro, *cyber crime*³³⁰.

Le prime attività concrete che andavano verso una cooperazione europea in materia penale sono state svolte dal Gruppo TREVI³³¹. Non a caso, col Trattato di Maastricht l'attività di questo venne assorbita nel terzo pilastro relativo alla cooperazione giudiziaria e di polizia in materia penale.

Con l'Accordo di Schengen e con l'Atto Unico Europeo (AUE)³³² i tempi erano ormai maturi per dare alla luce la cooperazione giudiziaria in materia penale nell'ambito

individuare *ex ante* quel giudice che il legislatore vuole competente, garantendo in pieno un giudice terzo ed imparziale. La competenza, quindi, si radica una volta applicati i criteri individuati dal legislatore a quel determinato fatto così come rilevato dalle indagini e ormai immutabile in giudizio. Diverso discorso, invece, per la legittimazione: l'ufficio del Pubblico Ministero svolge le indagini, ossia un'attività *in fieri* volta all'individuazione di fatti, soggetti ed elementi relativi ad un fatto-reato da accertare in giudizio. Per questo motivo non potrebbe parlarsi di competenza, bensì di legittimazione. Infatti, la legittimazione dell'ufficio del Pubblico Ministero si individua attraverso una valutazione prognostica mediante l'applicazione delle regole della competenza per il giudice che sarà investito di quel determinato processo. Si tratterebbe, dunque, di una individuazione *per relationem* dell'ufficio del Pubblico Ministero legittimato. Non sarebbe, quindi, un criterio cristallizzato, ma mobile e modificabile in virtù dei nuovi risultati delle indagini che potrebbero comportare una variazione della legittimazione, poiché trattasi ancora di una fase investigativa, dove l'ufficio del Pubblico Ministero svolge una funzione inquirente. Tale teoria è dimostrata attraverso una interpretazione sistematica degli artt. 25, 102, 104, 111, 112 Cost., degli articoli del libro I capo II c.p.p. e degli artt. 50 e 51 c.p.p. È necessario, però, validare tale teoria anche applicandola alle norme del diritto dell'Unione Europea. Poiché i testi legislativi europei utilizzano tale terminologia, l'interpretazione letterale porterebbe verso l'utilizzo del termine competenza. Se però si legge attentamente l'art. 86 TFUE si nota come vige il principio di primazia della Procura Europea sulle Procure nazionali affinché si rafforzi l'effettività della Procura Europea, creando così una struttura a livelli basata sul principio di sussidiarietà. Solo questo basterebbe a dimostrare come sia più opportuno utilizzare il termine legittimazione. Restano comunque alcune perplessità e la questione potrebbe aprire un dibattito in dottrina. Va considerato che la competenza resta prerogativa del giudice in quanto caratteristica rinvenibile unicamente nel processo. È solo con il processo, e non anche con la fase procedimentale, che si può parlare di competenza, perché solo qui è possibile individuare un giudice con giurisdizione piena. Per un approfondimento sul tema, si rimanda a L. CAMALDO, *La nuova fisionomia della procura europea all'esito del semestre di presidenza italiana del Consiglio europeo*, in *Cass. pen.*, 2, 2015, p. 0804B.

³³⁰ Cfr., P. BILANCIA, *Lo spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria*, in *Riv. It. Dir. pubbl. comunit.*, 2, 2004, p. 349 ss.

³³¹ Costituito nel 1975, riuniva i Ministri dell'interno degli Stati membri, e successivamente i Ministri della giustizia, su iniziativa del ministro degli esteri del Regno Unito Mr. Callaghan e presieduta dal membro olandese Mr. Fonteijn. Il gruppo aveva il compito di combattere il terrorismo, svolgere attività di contrasto alla criminalità e allo spaccio di sostanze stupefacenti, provvedere all'ordine pubblico e coordinare le attività di polizia, attesa l'incapacità di Interpol in tale campo. L'acronimo TREVI sta per terrorismo, radicalismo, estremismo e violenza internazionale. Non mancano, tuttavia, voci che attribuiscono il nome alla rinomata fontana romana, città nella quale si tenne la prima riunione. Cfr., G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all'ordine di indagine*, cit., p. 2; T. BUNYAN, *Trevi, Europol and European state*, in *Statewatching the new europe*, 1993, p. 1 ss.; G. GRASSO, *La cooperazione giudiziaria in materia penale tra gli Stati membri delle Comunità europee*, in *Foro it.*, 4, 1987, p. 458 ss.; A. DE GUTTRY, *La circolazione transnazionale delle informazioni tra organi inquirenti su fatti di terrorismo*, in AA.VV., *Europa e terrorismo internazionale* (a cura di N. RONZITTI), Milano, 1992, p. 46 ss.; P. LE JEUNE, *La coopération policière européenne contre le terrorisme*, Bruxelles, 1992; B. NASCIBENE, *Da Schengen a Maastricht: apertura delle frontiere, cooperazione giudiziaria e di polizia*, Milano, 1995, p. 16; S. NUTTAL, *European Political Cooperation*, Oxford, 1992, p. 300 ss.; A. PASQUERO, *Mutuo riconoscimento delle decisioni penali: prove di federalismo. Modello europeo e statunitense a confronto*, Milano, 2007, p. 4 ss.

³³² L'Atto Unico Europeo, firmato a Lussemburgo il 17 febbraio 1986, è stato ratificato in Italia con l. 23 dicembre 1986, n. 909 ed è entrato in vigore il 1° luglio 1987. L'AUE modifica i trattati delle Comunità

europeo, grazie anche all'introduzione del Sistema di informazione di Schengen³³³, strumento giuridico vincolante di promozione della cooperazione tra le forze di polizia e le amministrazioni doganali. Il preambolo dell'AUE, invece, consacrava espressamente la volontà degli Stati membri di attuare un'Unione europea che espandesse la propria competenza nei campi della sicurezza comune e della politica estera.

Si arrivava così alla nascita della cooperazione giudiziaria con il Trattato di Maastricht, il quale nel terzo pilastro disciplina la cooperazione giudiziaria e di polizia in materia penale (GAI).

Il Trattato di Maastricht non aveva inserito la cooperazione giudiziaria in materia penale nel primo pilastro e quindi non lo aveva comunitarizzato. Gli Stati membri preferirono semplicemente istituzionalizzarlo, ancorando le scelte al metodo intergovernativo in modo tale da adottare le decisioni ad unanimità³³⁴. Al fenomeno mancavano ancora i caratteri di incisività, democraticità e trasparenza dell'azione dell'Unione Europea.

Intanto con il Trattato di Amsterdam il terzo pilastro veniva riformato. Grazie a tale trattato esso venne politicizzato e parzialmente "comunitarizzato"³³⁵, aprendo così la strada a nuove forme di cooperazione³³⁶.

L'obiettivo dichiarato era raggiungere «uno spazio di libertà, sicurezza e giustizia»³³⁷ in cui sia assicurata la libera circolazione delle persone insieme a misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima»³³⁸, aprendo così la strada ad un diritto

Europee, in particolare inserendo all'art. 8 A TCE il primo dei quattro principi costitutivi del mercato unico: la libera circolazione delle persone. Successivamente al mercato unico si aggiungeranno altri tre principi: la libera circolazione delle merci, dei servizi e dei capitali. L'AUE è stato preceduto da quattro importanti tappe che hanno portato alla sua firma: la dichiarazione solenne di Stoccarda del 19 giugno 1983; il progetto di trattato che istituisce l'Unione europea adottato dal Parlamento europeo il 14 febbraio 1984; il Consiglio europeo di Fontainebleu del 25 e 26 giugno 1984; il Libro bianco sul mercato interno del 1985 con cui sono individuati i provvedimenti legislativi necessari per completare il mercato interno.

³³³ Il Sistema di informazione Schengen è una banca dati con lo scopo di garantire che determinati soggetti ritenuti pericolosi non circolino liberamente all'interno del territorio europeo. Il sistema si basa su un meccanismo di segnalazioni trasmesse in senso orizzontale tra la direzione centrale con sede a Strasburgo (C-SIS) e le sezioni nazionali (N-SIS) con sede in ogni Stato fornendo in tempo reale le informazioni necessarie sulla persona segnalata all'autorità procedente. Lo scopo è quello di facilitare le comunicazioni tra le varie polizie nazionali in occasione dell'arresto di una persona. Il SIS si è evoluto successivamente in SIS II con la Decisione del Consiglio 533/2007/GAI che ha introdotto nuove categorie di dati conoscibili col sistema. Per un approfondimento sul tema si rimanda a P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 1099 ss.

³³⁴ In questi termini, R. ADAM, *La cooperazione nel campo della giustizia e affari interni: da Schengen a Maastricht*, in *Rivista di diritto europeo*, 1994, p. 225 ss.; A. TIZZANO, *Brevi note sul "terzo pilastro" del trattato di Maastricht*, in *Dir. Un. Eur.*, 2, 1996, p. 391.

³³⁵ Così, U. VILLANI, *Istituzioni di diritto dell'Unione europea*, Bari, 2017, p. 20.

³³⁶ L'osservazione è di L. SALAZAR, *La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il programma dell'Aja*, in *Cass. Pen.*, 11, 2004, p. 3510.

³³⁷ Sullo spazio di libertà, sicurezza e giustizia nel Trattato di Amsterdam si legga AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007, *passim*; AA.VV., *Lo spazio di libertà, sicurezza e giustizia* (a cura di U. DRAETTA, N. PARISI, D. RINOLDI), Napoli, 2007, *passim*.

³³⁸ Così nel *Piano d'azione del Consiglio e della Commissione sul modo migliore per attuare le disposizioni del Trattato di Amsterdam concernenti uno spazio di libertà, sicurezza e giustizia*, in G.U.C.E. n. C 019 del 23 gennaio 1999. In esso si specifica che le tre nozioni di libertà, sicurezza e giustizia hanno una stretta connessione tra loro, in quanto «la libertà perde fortemente di significato se essa non può essere vissuta in un ambiente sicuro e senza un sistema giudiziario che riscuota la fiducia dei cittadini dell'Unione

penale europeo che si sarebbe progressivamente sviluppato con il rafforzamento delle procedure di cooperazione e con il ravvicinamento delle legislazioni in materia penale degli Stati membri con l'obiettivo di fornire ai cittadini un livello elevato di sicurezza.

Intanto venivano creati nuovi organismi come i magistrati di collegamento e la Rete Giudiziaria europea (RGE)³³⁹ e si sviluppavano strumenti normativi come le decisioni quadro, più efficaci delle convenzioni precedenti, adottate in gran numero per armonizzare sia le norme di diritto penale sostanziale, sia le norme di diritto penale processuale³⁴⁰.

e delle persone che vi risiedono. Queste tre nozioni indissociabili hanno un denominatore comune – i cittadini – e ognuna di esse non può essere pienamente realizzata senza le altre due». La dottrina ha inoltre osservato che il concetto di “spazio” non abolisce il concetto di territorio nazionale, ma si aggiunge ad esso in modo tale da chiarire che i territori nazionali costituiscono un'unità geografica comune nell'Unione europea. Cfr., A. WEYEMBERGH, *Storia della cooperazione*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 214.

³³⁹ I magistrati di collegamento sono stati istituiti con l'Azione comune 96/277/GAI del 22 aprile 1996 adottata dal Consiglio dell'Unione Europea. L'obiettivo è quello di attuare uno scambio di magistrati o funzionari particolarmente esperti in procedure di cooperazione giudiziaria, sulla base di accordi bilaterali o multilaterali tra gli Stati membri al fine di accrescere la rapidità e l'efficacia della cooperazione giudiziaria e di contribuire allo scambio di informazioni sui sistemi giuridici giudiziari degli Stati membri e sul loro funzionamento.

La Rete Giudiziaria Europea (RGE) è istituita con Azione comune 98/428/GAI del 29 giugno 1998. Nata per migliorare sul piano giuridico e pratico, la cooperazione giudiziaria, specie per quanto riguarda la lotta contro le gravi forme di criminalità, è una rete di punti di contatto giudiziari tra gli Stati membri dell'Unione europea. Le autorità competenti mantengono la propria sede nel Paese di origine, ma svolgono un'attività di intermediazione tra le autorità nazionali e i punti di contatto esteri al fine di agevolare la cooperazione giudiziaria. Sul tema si legga G. DE AMICIS, *La cooperazione orizzontale*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 315 ss. Secondo la dottrina, la successiva istituzione di Eurojust ha consolidato a livello strutturale, organizzativo ed operativo quanto già avviato con i magistrati di collegamento e la Rete Giudiziaria europea, al fine di migliorare diversi aspetti della cooperazione giudiziaria in materia penale. Cfr., L. KALB, *Procedimenti «paralleli» e giurisdizione «concordata»: il nuovo quadro normativo sul trasferimento dei procedimenti penali (nello spazio europeo e in quello internazionale)*, in *Arch. pen.*, 1, speciale riforme, 2018, p. 799; L. PALMIERI, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, cit., p. 23.

³⁴⁰ Si pensi ad esempio alla decisione quadro del Consiglio 2001/200/GAI del 15 marzo 2001 sulla posizione della vittima nel procedimento penale e alla dir. 2004/CE del Consiglio del 29 aprile 2004, relativa all'indennizzo delle vittime di reato. Tra le decisioni quadro volte ad armonizzare i sistemi penali nazionali, vanno ricordate la decisione quadro del Consiglio 2001/413/GAI del 28 maggio 2001 sulla lotta contro le frodi e le falsificazioni dei mezzi di pagamento diversi dal denaro contante; la decisione quadro del Consiglio 2001/500/GAI del 26 giugno 2001 sul riciclaggio di denaro, individuazione, rintracciamento, congelamento o sequestro e confisca degli strumenti e dei proventi di reato; la decisione quadro del Consiglio 2002/475/GAI del 13 giugno 2002 in materia di lotta contro il terrorismo successivamente modificata dalla decisione quadro 2008/919/GAI che introduce, tra gli altri, gli obblighi di penalizzazione della pubblica istigazione a commettere tali reati; la decisione quadro del Consiglio 2002/629/GAI del 19 luglio 2002 sulla tratta di esseri umani; la decisione quadro del Consiglio 2002/946/GAI del 28 novembre 2002 sulla repressione penale del favoreggiamento dell'ingresso e del soggiorno illegali; la decisione quadro del Consiglio 2003/568/GAI del 22 luglio 2003 sulla lotta contro la corruzione nel settore privato; la decisione quadro del Consiglio 2004/68/GAI del 22 dicembre 2003 in tema di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia; la decisione quadro 2005/55/GAI sugli attacchi contro i sistemi di informazione; la decisione quadro 2008/913/GAI sulla repressione del razzismo e della xenofobia; la decisione quadro 2008/977/GAI sulla protezione dei dati personali nelle materie del terzo pilastro; la decisione quadro 2008/909/GAI sull'applicazione del principio del reciproco riconoscimento alle sentenze penali che irrogano pene detentive o comunque privative della libertà personale, ai fini della loro esecuzione nell'Unione Europea; la decisione quadro 2008/947/GAI sull'applicazione del principio del mutuo riconoscimento alle sentenze ed alle decisioni di sospensione condizionale, in vista della sorveglianza delle

Il cambio di rotta sul piano contenutistico e programmatico era chiaro: superare una visione strettamente mercantile e far coincidere uno spazio economico con uno spazio giuridico e giudiziario dove le persone, oltre a spostarsi liberamente, si sentano anche al sicuro grazie alle attività di contrasto e prevenzione delle gravi forme di criminalità nonché a procedure di accertamento dei reati che siano comunque garantiste e rispettose dei diritti fondamentali al fine di rafforzare, da un lato, la cooperazione giudiziaria e di polizia, dall'altro, di tentare di ravvicinare le normative penali degli ordinamenti nazionali³⁴¹.

Il 15 e 16 ottobre 1999 si teneva il vertice di Tampere, passo di fondamentale importanza per la realizzazione dello spazio giudiziario europeo poiché il Consiglio Europeo venne interamente dedicato a esso. Le conclusioni del documento programmatico rappresentano una svolta epocale per la cooperazione nell'Unione, poiché si individuano nuovi principi e nuovi obiettivi.

Tra i più rilevanti vi sono il principio del mutuo riconoscimento delle decisioni giudiziarie, definito “pietra angolare della cooperazione penale nell'Unione Europea”³⁴², il quale sarà poi espressamente previsto nel Trattato di Lisbona³⁴³; il principio del ravvicinamento delle legislazioni degli Stati membri attraverso la strategia del c.d. “doppio binario”; e il principio del coordinamento delle indagini, il quale porterà nel 2002 all'istituzione di Eurojust³⁴⁴.

misure e sanzioni alternative alla pena detentiva; la decisione quadro del Consiglio 2008/841/GAI del 24 ottobre 2008 relativa alla lotta contro la criminalità organizzata.

³⁴¹ Cfr. G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e *procedimento penale italiano* (a cura di L. KALB), cit., p. 511. Sul punto si veda anche M. PISANI, *Criminalità organizzata e cooperazione internazionale*, cit., p. 703 ss.

³⁴² Cfr. Conclusioni della Presidenza del Summit europeo di Tampere, 15 e 16 ottobre 1999, SN 200/99.

³⁴³ Cfr. l'art. 67 e l'art. 82 TFUE

³⁴⁴ Eurojust venne istituita con decisione del Consiglio 2002/187/GAI attuata in Italia con la L. 14 marzo 2005, n. 41. Esso consiste in un organismo europeo dotato di personalità giuridica indipendente dalle altre istituzioni comunitarie composto da procuratori, magistrati o funzionari di polizia di pari competenza e distaccati da ciascuno degli Stati membri d'Unione Europea. Il regolamento (UE) 2018/1727 istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust). Tale Agenzia sostituisce e succede all'Unità Eurojust istituita con la decisione 2002/187/GAI, rappresentando un unico quadro giuridico rinnovato previsto dal nuovo regolamento. Ruolo fondamentale di Eurojust è incentivare la cooperazione giudiziaria in materia penale, migliorare il coordinamento delle indagini, dei procedimenti e lo scambio di informazioni tra le autorità competenti degli Stati membri in ipotesi di forme gravi di criminalità transnazionale, in particolare la criminalità organizzata. Dunque, la collaborazione con le autorità e gli operatori nazionali risulta essere il pilastro del lavoro di tale organismo. Inoltre, Eurojust ha anche la facoltà di fornire assistenza nelle indagini e nei procedimenti che coinvolgono uno Stato membro ed uno Stato non membro, qualora sia stato concluso un accordo di cooperazione tra Eurojust e lo Stato non membro ovvero vi sia un interesse di carattere essenziale nell'offerta di tale assistenza. Per un approfondimento sulla funzione e struttura di Eurojust, prima del regolamento (UE) 2018/1727, si rimanda a G. CASELLI, G. DE AMICIS, *La natura di Eurojust e la sua attuazione nell'ordinamento interno*, in *Dir. e giustizia*, 2003, p. 94 ss.; G. NICASTRO, *Eurojust*, in AA.VV., *Diritto penale europeo e ordinamento italiano*, Milano, 2006, p. 63 ss.; M. CHIAVARIO, *Diritto processuale penale*, cit., p. 915 ss.; M.R. MARCHETTI, *Rapporti giurisdizionali con autorità straniere*, in AA.VV., *Compendio di procedura penale* (a cura di M. BARGIS), Milano, 2020, pp. 1030 ss.; G. DE AMICIS, *Gli organismi centralizzati della cooperazione giudiziaria: Eurojust*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 261 ss.; L. PALMIERI, voce *Eurojust*, in *Enciclopedia Treccani on line*, [http://www.treccani.it/enciclopedia/eurojust_\(Diritto-on-line\)/](http://www.treccani.it/enciclopedia/eurojust_(Diritto-on-line)/). Sul nuovo assetto di Eurojust assunto con il regolamento (UE) 2018/1727, L. PALMIERI, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, Milano, 2019; L. SALAZAR, *La riforma di Eurojust e i suoi riflessi sull'ordinamento italiano*, in *Dir. pen. cont.*, 1, 2019, p. 44 ss.; E. ZANETTI, *Nasce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale*, in *Proc. pen. e giust.*, 2, 2019, p. 302 ss. Sia, inoltre,

Seguivano poi il Programma dell'Aja adottato dal Consiglio il 5 novembre 2004, destinato a sostituire il programma di Tampere, e il Piano d'azione del 2005 per l'attuazione del Programma dell'Aja al fine di rafforzare la libertà, la sicurezza e la giustizia nell'Unione europea. Questi chiariscono ulteriormente il concetto di spazio penale europeo e confermano la rilevanza del principio del mutuo riconoscimento e della fiducia reciproca, stabilendo dieci obiettivi, tra cui uno relativo alla circolazione della prova ed uno relativo al miglioramento e facilitazione della "cooperazione rafforzata"³⁴⁵.

Nonostante i numerosi tentativi di armonizzazione, lo spazio giudiziario europeo continuava a essere inadeguato sotto due profili: da una parte, i meccanismi operativi possedevano limitati poteri, con conseguenti seri problemi relativi alle prospettive di ravvicinamento delle legislazioni penali; dall'altra, gli Stati continuavano a resistere agli obiettivi fissati dall'Unione europea, bloccando l'emanazione delle decisioni quadro e resistendo all'attribuzione di ulteriori segmenti della loro sovranità.

Il Trattato di Lisbona modificava definitivamente e radicalmente l'assetto dell'Unione europea³⁴⁶. Vaniva abolito il terzo pilastro ed escluso il metodo intergovernativo. Al suo posto veniva implementato il metodo comunitario, il quale prevede la procedura legislativa ordinaria e l'adozione di Regolamenti e direttive attraverso il meccanismo di co-decisione tra Parlamento europeo e Consiglio. Le decisioni-quadro già emanate non restano "*flatus vocis*"³⁴⁷, ma mantengono vigore fino a quando non saranno oggetto di apposita revisione o abrogazione in base alle procedure legislative disciplinate dal TFUE. Pertanto, sono destinate ancora ad essere implementate in ordinamenti nazionali.

consentito il rinvio ad A. GAUDIERI, *La nuova Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust)*, in *Osservatorio SLSG*, novembre 2018, consultabile al link: <https://www.unisa.it/uploads/14394/audieri.nov.2018.pdf>.

³⁴⁵ Per un'ampia trattazione del tema si veda G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007, p. 465 ss.; L. SALAZAR, *Presente e futuro dello Spazio di libertà, sicurezza, e giustizia: dal Piano d'azione dell'Aja alla "visione" della Commissione europea*, in AA.VV., *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale* (a cura di G. GRASSO, R. SICURELLA), Milano, 2008, pp. 625 ss.

È possibile individuare i dieci obiettivi leggendo la Comunicazione della Commissione al Consiglio e al Parlamento europeo, del 10 maggio 2005 – Il programma dell'Aja: dieci priorità per i prossimi cinque anni. Partenariato per rinnovare l'Europa nel campo della libertà, sicurezza e giustizia, in G.U.U.E. n° C 236 del 24 settembre 2005.

³⁴⁶ In argomento, E. APRILE, L. DANIELE, *Cooperazione giudiziaria penale nell'Unione europea prima e dopo il Trattato di Lisbona*, Milano, 2009; S. CIVATARESE MATTEUCCI, F. GUARRIELLO, P. PUOTI, *Diritti fondamentali e politiche dell'Unione europea dopo Lisbona*, Rimini, 2013; L. DANIELE, *Trattato di Lisbona: addio all'idea federalista per superare gli ostacoli degli euroscettici*, in *Guida. Dir.*, 6, 2007, p. 11 ss.; A. GIARDA, *Un decennio di giustizia penale europea prima del Trattato di Lisbona*, in AA.VV., *I nuovi orizzonti della giustizia penale europea*, Atti del convegno ASPP, Milano, 24-26 ottobre 2014, Milano, 2015, p. 29 ss.; G. TIBERI, *Le nuove fonti del diritto nella cooperazione giudiziaria in materia penale dopo il Trattato di Lisbona e il loro impatto interno*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), cit., p. 13 ss.; V. PATANÈ, *Il processo penale nei nuovi scenari dello spazio di libertà, sicurezza e giustizia dell'Unione europea*, in AA.VV., *L'Unione europea dopo il Trattato di Lisbona* (a cura di N. PARISI, V. PETRALIA), Torino, 2011, p. 143 ss.

³⁴⁷ L'espressione è tradizionalmente attribuita al filosofo medievale Roscellino di Compiègne (morto intorno al 1120), massimo rappresentante del nominalismo medievale, secondo il quale i concetti universali non hanno alcuna realtà oggettiva e sono soltanto semplici nomi (cioè, appunto, dei *flatus vocis*). È talora ripetuta nel linguaggio comune, riferita in senso polemico a discorsi privi di consistenza o a promesse che non hanno seguito.

La politica perseguita dall'Ue nel post-Lisbona è volta a sostituire gradualmente e a sostituire le decisioni-quadro, cardini del vecchio terzo pilastro, con altrettante direttive. Questa opera di revisione è proceduta all'inizio lentamente, per poi ricevere una seria accelerazione: sono tantissimi gli atti del vecchio terzo pilastro relativi a cooperazione in materia penale tradotti in direttive, anche se tale lavoro non può dirsi ancora concluso.

La cooperazione giudiziaria diventa un obiettivo primario incluso nella più grande macro-area dello Spazio di libertà, sicurezza e giustizia. In questo modo è stata razionalizzata l'intera struttura e sono stati risolti tutti i problemi relativi ai settori "transpilastro", cioè a quelle materie che trovavano regolamentazione in più settori e che avevano reso difficile l'applicazione delle norme europee.

L'azione dell'Unione europea risulta non solo semplificata ma anche rafforzata, in quanto più coerente e chiara. Diverso discorso, invece, dovrà farsi in merito alla produzione normativa che ne è derivata.

L'eliminazione del terzo pilastro ha consentito l'applicazione dei principi generali del diritto comunitario tra cui il principio di leale collaborazione, dell'obbligo di interpretazione conforme, e della supremazia del diritto dell'Unione anche alla cooperazione giudiziaria e di polizia in materia penale³⁴⁸, nonché ha ampliato il controllo giudiziario, estendendolo alla Corte di giustizia dell'Unione europea che può pronunciarsi in via pregiudiziale sui ricorsi per infrazione, per annullamento, per carenza e per risarcimento³⁴⁹. Devono, quindi, esser rispettati non solo i diritti fondamentali dei differenti sistemi statuali, ma anche i diritti e i principi generali dell'ordinamento europeo, come il principio di proporzionalità e di sussidiarietà³⁵⁰.

In virtù delle sfide del nuovo millennio, dello sviluppo sociale, culturale, economico e alla luce delle nuove esigenze dei cittadini europei, il Trattato di Lisbona ha dovuto creare una nuova base solida per lo sviluppo di uno spazio di giustizia penale, dando nuovi e più incisivi poteri al Parlamento europeo. Si sta procedendo, quindi, verso lo sviluppo di uno spazio comune di giustizia penale che rinviene alla base il principio del reciproco riconoscimento.

La dottrina nota come la tensione del Trattato di Lisbona verso l'armonizzazione progressiva e il ravvicinamento della normativa tra Paesi membri dell'Unione europea, che risponde all'obiettivo di creare una normativa comune, funga anche da stimolo alla promozione e diffusione di una cultura volta allo sviluppo dei diritti fondamentali e

³⁴⁸ Sul punto, R.E. KOSTORIS, *Processo penale e paradigmi europei*, Torino, 2018, p. 164 ss. Secondo l'A. il diritto dell'Unione europea sarebbe figlio di una società pluralista e liquida, tant'è che con l'abolizione del Terzo pilastro e la comunitarizzazione della cooperazione giudiziaria e di polizia in materia penale si sarebbe verificato una contaminazione del sistema giudiziario interno che rischia di generare una «delegificazione per trascinarsi», con la conseguente genesi di un nuovo fenomeno, quale l'induzione dei giudici a dar minor rilievo alle regole della normativa intera rispetto al passato.

³⁴⁹ Così, A. DI STASI, *Spazio europeo di libertà, sicurezza e giustizia e cooperazione giudiziaria in materia penale: il rispetto dei diritti fondamentali e delle diversità tra ordinamenti nazionali e tradizioni giuridiche*, in AA.VV., *«Spazio europeo di giustizia» e procedimento penale italiano* (a cura di L. KALB), cit., p. 3 ss.

³⁵⁰ In tema, F. BUONOMENNA, *Profili evolutivi di sussidiarietà europea e di sovranità inclusiva*, in *Rivista della cooperazione giuridica internazionale*, 56, 2017, p. 153 ss.; S. MONTALDO, *Amici mai, odiarsi mai: il controllo sull'applicazione del principio di sussidiarietà alla luce della prassi della Commissione e della Corte di giustizia*, in *Federalismi.it*, 26 giugno 2016, p. 2 ss., disponibile al link: <https://www.federalismi.it/ApplyOpenFilePDF.cfm?artid=32110&dpath=document&dfile=27062016110654.pdf&content=Il%2Bcontrollo%2Bsull%27applicazione%2Bdel%2Bprincipio%2Bdi%2Bsussidiariet%C3%A0%2B%2D%2Bstato%2B%2D%2Bdottrina%2B%2D%2B>

all'affermazione delle garanzie contenute nella Convenzione europea dei diritti dell'Uomo³⁵¹.

Infatti, la facilitazione della cooperazione giudiziaria in materia penale tra i Paesi membri e il rafforzamento del principio di reciproco riconoscimento avrebbe creato un circolo virtuoso che incoraggia la diffusione dei diritti fondamentali e addirittura favorisce l'ampliamento di questi³⁵². Tutto ciò è confermato dal fatto che si è sviluppata una costellazione di direttive che tengono pienamente conto dei principi fondamentali dell'Unione europea consacrati anche nella Convenzione europea dei diritti dell'Uomo, così come interpretati dalla Corte di Strasburgo³⁵³.

In merito al contenuto delle attività di cooperazione, il Trattato ha inciso fortemente sul principio del mutuo riconoscimento delle sentenze e delle decisioni giudiziarie, sull'individuazione di basi giuridiche comuni per ravvicinare le legislazioni, sul rafforzamento dei poteri di Europol e Eurojust, sulla costituzione del Procuratore europeo³⁵⁴, ed infine sul settore relativo alla circolazione probatoria transnazionale³⁵⁵.

Il processo evolutivo sinora descritto è ricco di mutamenti repentini e radicali avvenuti in un brevissimo arco temporale. Tutto ciò ha creato numerosi *deficit* nel sistema europeo a partire dalle soluzioni di compromesso che sono state adottate pur di rintracciare il consenso di tutti gli Stati membri. Si nota, *prima facie*, un gran numero di grossolane modifiche all'assetto strutturale e funzionale della cooperazione. Si pensi all'enorme e confusionale produzione normativa susseguitasi nel tempo sotto la forma prima di decisioni quadro e poi di direttive e Regolamenti.

³⁵¹ Per un commento sul rapporto tra la Convenzione europea dei diritti dell'Uomo e la cooperazione giudiziaria penale si veda, *ex multis*, S. NEGRI, *L'incidenza della Convenzione europea dei diritti dell'Uomo sulla cooperazione giudiziaria penale nell'Unione europea*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali, (a cura di L. KALB), cit., p. 55 ss.; ID., *La realizzazione dello spazio europeo di libertà, sicurezza e giustizia tra Carta dei diritti fondamentali e CEDU: dalla convergenza alla integrazione tra sistemi?*, in AA.VV., *Spazio europeo e diritti di giustizia. Il capo VI della Carta dei diritti fondamentali nell'applicazione giurisprudenziale* (a cura di A. DI STASI), Napoli, 2014, p. 111 ss.; E. APRILE, *La tutela dei diritti fondamentali e le nuove garanzie del processo penale*, in AA.VV., *Cooperazione giudiziaria penale nell'Unione europea prima e dopo il Trattato di Lisbona*, (a cura di E. APRILE-F. SPIEZIA), Milano, 2009, p. 117 ss.; L. KALB (a cura di), *Mandato d'arresto europeo e procedure di consegna. Commento alla legge 22 aprile 2005, n.69*, Milano, 2005.

³⁵² Sul punto si legga S. NEGRI, *L'incidenza della Convenzione europea dei diritti dell'uomo sulla cooperazione giudiziaria penale nell'Unione Europea*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano, cit., p. 63 ss.

³⁵³ Si pensi, a titolo esemplificativo, alla direttiva 2010/64/UE sul diritto all'interprete e al traduttore nei procedimenti penali in GUUE, L 280 del 26 ottobre 2010, o alla direttiva 2012/13/UE sul diritto all'informazione nei procedimenti penali in GUUE, L 142 del 1° giugno 2012, o ancora alla direttiva 2011/99/UE sull'ordine di protezione europeo in GUUE, L 338 del 21 dicembre 2011. Per un approfondimento su tali direttive si rimanda a L. KALB, I. IZZO, *La nuova sfida della direttiva 2010/64: un'assistenza linguistica di "qualità" per lo svolgimento di un procedimento effettivamente "equo"*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano, cit., p. 344 ss. Per un commento critico a una decisione giurisprudenziale ove si conferma i limiti alla piena operatività del diritto all'assistenza linguistica presenti nella prassi, L. KALB, *L'effettività del diritto alla traduzione degli atti dopo la Dir. 2010/64/UE*, in *Giur. It.*, 1, 2014, p. 714 ss. Sull'ordine europeo di protezione, A. MARANDOLA, *L'ordine di protezione europeo*, in *Studium Iuris*, 9, 2015, p. 989 ss.

³⁵⁴ Così, F. SPIEZIA, *La cooperazione giudiziaria internazionale e lo spazio di giustizia europeo*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), cit., p.867 ss.

³⁵⁵ Si vedano gli art. 82 ss. TFUE.

Si auspica che il legislatore europeo avvii una seria opera di “revisione” e di “razionalizzazione” dell’intera produzione normativa, evitando il rischio di confusioni e sovrapposizioni normative che generano un sistema incomprensibile, tortuoso, ricco di norme intricate.

Un ulteriore passo veniva compiuto con il Programma di Stoccolma³⁵⁶ e con il Piano d’azione³⁵⁷ che lo attua. Il Consiglio europeo, composto da capi di Stato e di governo degli Stati membri, si riunì il 10 e 11 dicembre 2009 per stabilire il nuovo programma quinquennale 2010-2014 seguendo quanto stabilito dalla *road map* successivamente precisata nel Piano d’azione presentato dalla Commissione il 20 aprile 2010.

La tabella di marcia individuava sei ambiti principali nei quali sono auspicabili iniziative legislative o di altro tipo: traduzione e interpretazione; informazioni relative ai diritti e all’accusa; consulenza e assistenza a livello legale; comunicazione con familiari, datori di lavoro e autorità consolari; garanzie speciali per indagati o imputati vulnerabili; detenzione preventiva³⁵⁸.

Il Programma di Stoccolma, sulla scia dei risultati raggiunti dai programmi di Tampere e dell’Aja, mirava ad accogliere le nuove sfide e a rafforzare lo sviluppo dello spazio europeo di libertà, sicurezza e giustizia con azioni concentrate sugli interessi e sulle esigenze dei cittadini che vivono in tale area, rendendo effettivi gli strumenti già esistenti e proponendone la creazione di nuovi più incisivi. Per la prima volta si assiste ad uno stretto collegamento tra un Programma e il Trattato di Lisbona, punto di riferimento per l’azione dell’Unione europea, confermato anche dai continui riferimenti ai diritti fondamentali³⁵⁹.

In realtà, c’è chi fa notare come il Programma di Stoccolma abbia creato un progetto fin troppo ambizioso per quanto riguarda i meccanismi di cooperazione e il ravvicinamento delle legislazioni. Sotto molti aspetti il Programma è stato ritenuto superficiale nell’individuazione sia degli obiettivi, sia delle modalità per realizzarli. Il

³⁵⁶ In GUUE, C 115 del 4 maggio 2010.

³⁵⁷ COM (2010) 171 final, 20 aprile 2010.

³⁵⁸ Nell’ottobre 2010 il Parlamento e il Consiglio hanno adottato una direttiva sul diritto all’interpretazione e alla traduzione nei procedimenti penali (direttiva 2010/64/UE). Nel maggio 2012 il Parlamento e il Consiglio hanno adottato la direttiva 2012/13/UE sul diritto all’informazione nei procedimenti penali (la cosiddetta «comunicazione dei diritti»). Nell’ottobre 2013 il Parlamento e il Consiglio hanno adottato la direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore nel procedimento penale e al diritto di comunicare al momento dell’arresto. Nel giugno 2011 la Commissione ha pubblicato un Libro verde sull’applicazione della normativa dell’UE sulla giustizia penale nel settore della detenzione. Nel dicembre 2011 il Parlamento ha approvato una risoluzione in cui chiede standard comuni a livello di UE sulle condizioni di detenzione. Il 27 novembre 2013 la Commissione ha presentato un pacchetto di proposte legislative a completamento della tabella di marcia sulle garanzie procedurali. Nel marzo 2016 il Parlamento e il Consiglio hanno adottato la direttiva (UE) 2016/343 sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali. Nel maggio 2016 il Parlamento e il Consiglio hanno adottato la direttiva (UE) 2016/800 sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali, mentre il 26 ottobre 2016 l’Unione europea ha adottato la direttiva (UE) 2016/1919 sull’ammissione l’ammissione al patrocinio a spese dello Stato per indagati e imputati nell’ambito di procedimenti penali e per le persone ricercate nell’ambito di procedimenti di esecuzione del mandato d’arresto europeo.

³⁵⁹ In tal senso si legga F. SPIEZIA, *La cooperazione giudiziaria internazionale e lo spazio di giustizia europeo*, cit., p. 844 ss. Per un confronto si legga anche M. CAIANIELLO, *Dal Terzo pilastro ai nuovi strumenti: diritti fondamentali, “road map” e l’impatto delle nuove direttive*, in AA.VV., *I nuovi orizzonti della giustizia penale europea*, Atti del convegno ASPP, Milano, 24-26 ottobre 2014, Milano, 2015, p. 97 ss.; F. DE ANGELIS, *L’espace judiciaire Pénal Européen: une vision se concrétise*, in *ERA Forum*, 1, supplement, 2011, p. 43 ss.; T. RAFARACI, *La cooperazione di polizia e giudiziaria in materia penale nell’Unione Europea dopo il Trattato di Lisbona*, Milano, 2011.

tutto è stato poi aggravato da un piano d'azione accolto freddamente dal Consiglio in quanto eccedeva nello sviluppo di aspetti che il Programma non conteneva, mentre dall'altra parte non teneva in debito conto gli obiettivi evidenziati dal Consiglio³⁶⁰.

Forte attenzione è data al ravvicinamento degli ordinamenti nel campo della procedura penale: si confermava con forza il principio del riconoscimento reciproco in materia penale e si prevedeva un nuovo strumento, finalizzato alla formazione di prove caratterizzate dalla transnazionalità, comune a tutti i Paesi nonché una nuova disciplina per la difesa delle vittime e per la tutela dei diritti degli indagati e degli imputati.

In effetti, per il Consiglio appare da sempre rilevante il ruolo del principio di ravvicinamento delle normative degli Stati membri nell'instaurazione di uno spazio di giustizia europeo con *standard* minimi di tutela dei diritti individuali affinché si garantisca a pieno la libera circolazione ed esecuzione delle decisioni giudiziarie in ogni Stato membro.

Tale principio, infatti, è cardine del sistema intorno al quale ruotano gli obiettivi fissati, necessari per realizzare uno spazio di giustizia europeo. Si deve, quindi, dedurre che tra il principio di ravvicinamento delle normative degli Stati membri e gli obiettivi fissati per la realizzazione dello spazio di giustizia europeo ci sia un rapporto di mezzo/risultato, o se si preferisce di causa/effetto, dove il principio diventa il mezzo o la causa per realizzare il risultato o l'effetto "spazio di giustizia europeo". In mezzo invece si colloca il principio del riconoscimento reciproco delle decisioni giudiziarie e del mutuo scambio di informazioni e elementi di prova, realizzabili solo attraverso una seria e convinta applicazione del principio del ravvicinamento delle legislazioni tra Paesi membri.

Proprio il ravvicinamento delle legislazioni e il rafforzamento del principio del mutuo riconoscimento ha stimolato la proposta di nuove iniziative normative relative alla formazione della prova, in sostituzione delle vecchie norme, ormai obsolete e frammentarie³⁶¹. La normativa, secondo quanto stabilito dal Programma, dovrebbe contenere e rafforzare il principio del riconoscimento reciproco e rendere più semplice ed elastica la procedura tra Stati membri, accorciando i tempi, nel rispetto anche del principio della ragionevole durata del processo. Ulteriore elemento di novità sta nel prevedere l'estensione di tale strumento ad un numero maggiore di mezzi di prova, molti dei quali erano esclusi dal vecchio sistema previsto dal mandato europeo di ricerca della prova, al fine anche di migliorare i rapporti e lo scambio di informazioni tra le autorità degli Stati membri e tra questi e gli organismi europei. Particolare attenzione va destinata alle informazioni elettroniche.

Il programma si pone quali obiettivi prioritari lo sviluppo di una strategia di sicurezza interna dell'Unione per garantire la protezione dei cittadini e combattere la criminalità organizzata e il terrorismo nel pieno rispetto dei principi fondamentali dell'uomo.

Applicando il principio di solidarietà e di sussidiarietà, il programma vuole rafforzare la cooperazione giudiziaria in materia penale in settori particolarmente delicati e sensibili ritenendolo l'unico strumento a base comune (o comunque il più efficace) per combattere in maniera decisa i fenomeni di grave criminalità.

A tal fine, il Consiglio europeo ha invitato le autorità competenti degli Stati membri a valersi il più possibile degli strumenti europei messi a loro disposizione come le squadre

³⁶⁰ Sul punto, si legga il pensiero di A. WEYEMBERGH, *Storia della cooperazione*, cit., p. 228.

³⁶¹ Cfr. G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano, cit., p. 534.

investigative comuni, Eurojust ed Europol, il tutto basato su un reciproco scambio di informazioni.

La dottrina ha osservato come per l'applicazione dei principi fissati dal Programma di Stoccolma sia fondamentale la fiducia e un'armonizzazione tesa all'interazione, senza sfociare in contrapposizione o sovrapposizione dell'una sull'altra³⁶². Allora anche questi diventano criteri ispiratori per una efficace lotta alla criminalità, tesa alla sicurezza dei cittadini europei.

Si va così delineando un embrione di procedimento penale europeo con proprie caratteristiche e propri obiettivi, con un proprio territorio di applicazione e con regole specifiche, con organismi autonomi e del tutto originali, con propri soggetti, strumenti e addirittura con proprie sanzioni specifiche, in ossequio ai principi fondamentali dell'uomo, nel rispetto innanzitutto della dignità umana.

Ultimo passo politico verso una cooperazione giudiziaria più matura e stabile è compiuto con il Consiglio europeo del 26 e 27 giugno 2014 tenutosi a Ypres, in Belgio. Le conclusioni³⁶³ di tale Consiglio, però, si allontanano nettamente dal precedente Programma di Stoccolma. Infatti, il nuovo piano pluriennale è ritenuto non solo generico e sintetico, ma anche poco ambizioso rispetto agli obiettivi fissati in passato³⁶⁴. Altra parte della dottrina, di diverso avviso, ritiene che il documento sia in netta continuità con i precedenti programmi ed in particolar modo con il Programma di Stoccolma³⁶⁵. Il Consiglio delinea le nuove strategie per lo spazio europeo di libertà, sicurezza e di giustizia valevole per il quinquennio 2015-2020, dando un impulso e una linea politica necessari per lo sviluppo dell'Unione europea.

Ciò sembra avallato anche dal nome dato alle conclusioni: non più programma come furono denominati i documenti di Tampere, de l'Aja e di Stoccolma, ma semplici *strategic guidelines*, quasi ad indicare qualcosa di minor importanza rispetto al passato.

In realtà bisognerebbe tener conto di tutti i fattori intervenuti negli anni per comprendere tale scelta: molti Paesi non hanno ancora dato attuazione (o l'hanno fatto da poco) alle direttive indicate dalla *road map*. Inoltre, l'attenzione dell'Unione si è spostata progressivamente verso lo sviluppo di strategie per limitare gli effetti negativi della crisi economica, e non da ultimo bisogna rilevare che in passato, comunque, l'attività in tema di cooperazione giudiziaria è stata fiorente e prolifica, per cui sembra quasi fisiologico un leggero, seppur significativo, calo di attenzione verso la materia, che resta e resterà comunque di importanza primaria per l'Unione europea³⁶⁶.

A prova di tutto ciò basti notare qual è la priorità posta dal Consiglio: consolidare gli strumenti giuridici e le misure esistenti; adottare nuove misure con il solo scopo di armonizzare e rendere chiara la legislazione dell'Unione; proseguire nell'opera di implementazione dei diritti degli indagati ed imputati; rafforzare la normativa a tutela

³⁶² M. CHIAVARIO, *Giustizia europea e processo penale: nuovi scenari e nuovi problemi*, in *Leg. pen.*, 2008, p. 468.

³⁶³ Contenute in GUUE, C 240 del 24 luglio 2014.

³⁶⁴ Il riferimento è a A. WEYEMBERGH, *Storia della cooperazione*, cit., p. 228 ss.

³⁶⁵ Cfr., E. COTTU, *Il Consiglio Europeo adotta i nuovi orientamenti strategici per lo spazio di libertà, sicurezza e giustizia per il quinquennio 2015-2020*, in *Diritto Penale Contemporaneo*, 24 luglio 2014, disponibile al sito <http://www.penalecontemporaneo.it>.

³⁶⁶ A. WEYEMBERGH, *Storia della cooperazione*, cit., p. 229. Per un approfondimento sui decreti di recepimento delle direttive si rimanda a G. DI PAOLO, *Lo spazio di libertà, sicurezza e giustizia dell'UE: recenti novità sul fronte domestico e a livello europeo*, in *Cass. pen.*, 7/8, 2016, p. 3018C; M. GNES, E. CHITI, *Cronache europee 2015*, in *Riv. trim. dir. pubbl.*, 4, 2016, p. 1113; M. GNES, E. CHITI, *Cronache europee 2014*, in *Riv. trim. dir. pubbl.*, 3, 2015, p. 1047.

delle vittime; arrivare all’istituzione della Procura Europea, accrescendo di conseguenza le competenze di Eurojust ed Europol; incrementare l’impiego del principio del mutuo riconoscimento e dello strumento dello scambio di informazioni.

Seppur con i limiti sopra indicati, è lodevole l’obiettivo fissato dal Consiglio di rivedere e sistemare l’intera produzione normativa dell’Unione in un’ottica di maggior chiarezza e comprensione della legislazione europea.

Ulteriore conferma della genericità degli argomenti trattati dal Consiglio sono ravvisabili anche dalla struttura delle conclusioni: solo sei pagine rispetto alle trentotto del programma di Stoccolma. Anche il contenuto è fortemente scarno, povero di approfondimenti, e addirittura incapace di dare un vero e proprio orientamento per la normativa europea in campo penale. Infatti, unico dato interessante sembra essere la lotta più incisiva contro il traffico e la tratta di esseri umani e la lotta alla migrazione irregolare.

Per quanto riguarda, invece, gli altri obiettivi fissati, si nota come questi non siano idonei a dare un forte e decisivo impulso alla politica criminale europea rispetto a quanto fatto nei precedenti programmi: il Consiglio di Ypres non apre spazi a nuove e innovative soluzioni, ma si limita semplicemente a chiedere un rafforzamento degli strumenti e della normativa del passato.

Parte della dottrina non ha esitato a sottolineare come da tale situazione possano trarsi dei benefici come, ad esempio, un maggior intervento del Parlamento europeo in tale campo³⁶⁷, favorendo in tal modo il principio democratico e arrivando così alla piena applicazione del “metodo comunitario” anche all’ex terzo pilastro.

Nonostante la crisi politica dell’Unione europea, l’Europa della giustizia penale resta ancora oggi un cantiere aperto dove fervono i lavori relativi alla produzione normativa e giurisprudenziale con l’obiettivo di porre rimedio alle molteplici sfide sia del passato che del presente.

Lo conferma la recente Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell’UE per la lotta alla criminalità organizzata 2021-2025*³⁶⁸, con la quale la Commissione ritiene necessario: continuare nell’attività di promozione della cooperazione tra autorità di contrasto e autorità giudiziarie al fine di agevolare lo scambio di informazioni e permettere un accesso tempestivo alle informazioni; rendere le indagini più efficaci al fine di smantellare le strutture della criminalità organizzata e contrastare i reati altamente prioritari; eliminare gli utili generati dalla criminalità organizzata e prevenire l’infiltrazione dell’economia legale e nella società mediante il rafforzamento delle misure di recupero dei beni e di lotta al riciclaggio di denaro e il rafforzamento delle misure di lotta alla corruzione; adeguare i servizi di contrasto e del sistema giudiziario all’era digitale, favorendo il facile accesso agli indizi e alle prove digitali nonché lo sviluppo di strumenti e tecnologie efficaci.

Infine, uno sguardo va rivolto anche ai rapporti con il Regno Unito. Il traumatico abbandono dall’Unione europea consente comunque un rapporto di leale collaborazione, indice dell’insopprimibile necessità di proficue relazioni finalizzate al contrasto delle attività criminose internazionali.

Ed invero, con l’Accordo sugli scambi commerciali e la cooperazione tra l’Unione europea e la Comunità europea dell’energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall’altra, le parti hanno deciso di continuare a

³⁶⁷ Sul tema si legga E. COTTU, *Il Consiglio Europeo adotta i nuovi orientamenti strategici per lo spazio di libertà, sicurezza e giustizia per il quinquennio 2015-2020*, cit., *passim*.

³⁶⁸ COM (2021) 170 final, del 14 aprile 2021.

collaborare anche nei settori relativi alla cooperazione delle autorità di contrasto e giudiziarie in materia di prevenzione, indagine, accertamento e perseguimento di reati e di prevenzione e contrasto del riciclaggio di denaro e del finanziamento del terrorismo³⁶⁹.

5. Il principio della mutua assistenza e la progressiva riduzione della sua applicazione

La cooperazione giudiziaria in materia penale può basarsi sul principio di mutua assistenza ovvero sul principio del mutuo riconoscimento.

Come affermato nel “Libro verde sulla ricerca delle prove in materia penale tra Stati membri e sulla garanzia della loro ammissibilità”³⁷⁰, i due principi sviluppano modelli normativi differenti da poter utilizzare per la raccolta *ultra fines* e/o per il trasferimento dall'estero di fonti ed elementi di prova penali personali o reali.

Il “Libro verde” evidenzia correttamente come l'acquisizione delle prove sia incentrata su vari strumenti coesistenti basati sui due diversi principi. Questa impostazione rendeva gravosa l'applicazione delle norme e poteva ingenerare confusione tra gli operatori del diritto, che in alcuni casi non individuavano correttamente lo strumento più adeguato alla formazione della prova ricercata. Tali fattori rischiavano, in ultima analisi, di compromettere l'efficacia della cooperazione transfrontaliera.

Tra l'altro, gli strumenti basati sulla mutua assistenza possono essere considerati lenti e poco efficaci, in quanto non prevedono moduli *standard* da utilizzare per l'emissione della richiesta di acquisizione di prove che si trovano in un altro Stato membro né fissano i termini per la sua esecuzione. Gli strumenti basati esclusivamente sul mutuo riconoscimento, di contro, possono ritenersi insoddisfacenti a loro volta, poiché riguardano soltanto determinati specifici provvedimenti e prevedono numerosissimi motivi di rifiuto dell'esecuzione della decisione.

La mutua assistenza è il principio più risalente nel tempo. Essa si pone alla base del modello dell'“assistenza giudiziaria internazionale”³⁷¹, al quale si rifà anche il c.d. diritto convenzionale rogatorio.

Esso richiede il massimo rispetto delle norme relative alla ricerca e formazione delle prove dello Stato in cui la prova è reperibile, presupponendo un basso livello di integrazione dei sistemi processuali degli Stati interessati.

³⁶⁹ Per la disciplina dettagliata, v., Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra, ST/5198/2021/INIT, in GUUE, L 149 del 30 aprile 2021. Per un approfondimento sui rapporti tra Unione europea e Regno Unito a seguito della Brexit, L. SALAZAR, *La cooperazione giudiziaria penale nell'Unione ai tempi della Brexit*, in *Sistema penale*, 3, 2020, p. 185 ss.

³⁷⁰ COM (2009)624 def., dell'11 novembre 2009 della Commissione europea. L'obiettivo del Libro verde è consultare gli Stati membri e tutte le parti interessate in ordine a determinate questioni attinenti al tema della ricerca e ammissibilità delle prove in materia penale tra gli Stati membri. L'atto è consultabile all'indirizzo <http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52009DC0624>.

³⁷¹ Il termine “assistenza” deriva dal latino *adsistere* ed è utilizzato nel senso di “stare presso”, “stare accanto”. Quintiliano utilizza tale termine nel senso figurato di aiutare. Il termine rimanderebbe a una forma di supporto, di aiuto, proveniente dall'esterno, da qualcun altro nei confronti di chi ne ha bisogno. Invece il termine “cooperazione” deriva dall'unione della preposizione latina *cum* con il verbo *operari* e significa letteralmente “occuparsi con”. Il termine, quindi, rimanderebbe ad una attività svolta insieme ad altri per la realizzazione di un fine, ad una attività di collaborazione. L'assistenza giudiziaria internazionale prevede l'esperimento dell'attività da parte dello Stato richiesto, il quale segue le proprie regole, con il filtro di un organo giudiziario e politico.

Il trasferimento della prova avviene in base ad una cooperazione intergovernativa fra gli Stati interessati che intrattengono tra loro relazioni sia di carattere politico-amministrativo sia di carattere giudiziario secondo il modello del “doppio binario”, senza rapporti diretti tra autorità giudiziarie³⁷².

Il principio della mutua assistenza è il criterio tradizionalmente utilizzato dagli ordinamenti statuali in materia di cooperazione poiché assicura il massimo rispetto del “principio di sovranità” degli Stati e consente al singolo Stato di esercitare in maniera esclusiva lo *jus imperii* sul proprio territorio, in linea con quello che è il “principio di territorialità della giurisdizione”. Per questi motivi il principio della mutua assistenza giudiziaria è stato da sempre ritenuto da parte degli Stati «un modo per poter riaffermare, al di là delle frontiere, il potere di coazione dello Stato, la sua potestà sovrana»³⁷³.

Inoltre, l’attività estremamente facilitata delle autorità giudiziarie dello Stato in cui la fonte di prova è reperibile rappresenta un’ulteriore caratteristica ricollegabile al principio di sovranità, poiché consente loro di applicare le regole interne al proprio ordinamento giuridico³⁷⁴.

Volendo schematizzare, è possibile individuare tre elementi strutturali su cui si parametrizza il principio: il criterio del *locus regit actum*, lo schema della *richiesta*, e il “metodo intergovernativo”.

Il *locus regit actum* è il criterio fondante la mutua assistenza, secondo cui l’esecuzione dell’atto deve avvenire seguendo le regole del luogo in cui esso deve essere compiuto – ossia dello Stato richiesto – e ad opera delle autorità straniere competenti. Ricorrendo spesso nelle convenzioni sia bilaterali sia multilaterali, e stante la sua attitudine a essere rispettato, è ritenuto un principio generale “universalmente riconosciuto”³⁷⁵.

³⁷² In tal senso G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), cit., p. 534 ss.; M. DANIELE, *Ricerca e formazione della prova*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 458 ss.

³⁷³ Così, V. ESPOSITO, voce *Rapporti giurisdizionali con autorità straniere*, cit., p. 1.

³⁷⁴ Sul punto si veda B. PIATTOLI, *Rogatorie internazionali*, in AA.VV., *Rapporti internazionali* (a cura di M.G. AIMONETTO), Torino, 2002, p. 252; G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), cit., p. 537. Più in generale, sui principi generali di diritto riconosciuti dalle Nazioni civili, B. CONFORTI, *Diritto internazionale*, Napoli, 2014, p. 47 ss.; A. SINAGRA, P. BARGIACCHI, *Lezioni di diritto internazionale pubblico*, Milano, 2019, p. 156 ss.

³⁷⁵ Sul tema si veda Cass., Sez. I, sentenza del 22 ottobre 1981, n. 311, in *Giust. Pen.*, 3, 1982, p. 334, secondo la quale «costituisce principio di diritto internazionale universalmente riconosciuto quello secondo cui le rogatorie vanno eseguite secondo la legge dello Stato richiesto»; Cass., Sez. II, sentenza del 3 dicembre 1990, n. 7389, in *Cass. pen.*, 1992, p. 2795; Cass., Sez. VI, sentenza del 13 luglio 1999, n. 11109, in *Cass. pen.*, 2000, p. 3106, con nota di J.P. PIERINI, *Ancora attuale il principio locus regit actum con riguardo alle prove penali acquisite all'estero nel corso di rogatoria “concelebrata”?*, nonché, seppur in modo meno esplicito, Cass., Sez. VI, sentenza del 12 dicembre 2001, in *Cass. pen.*, 2002, p. 2859; Cass., Sez. II, sentenza del 22 dicembre 2016, n. 2173, ove la Suprema Corte ritiene il *locus regit actum* principio internazionale avente un unico limite: la prova non può essere acquisita in contrasto con i principi fondamentali dell’ordinamento giuridico italiano e dunque con il diritto di difesa. In dottrina, *ex multis*, M.R. MARCHETTI, *L’assistenza giudiziaria internazionale*, in AA.VV., *Trattato di procedura penale* (diretto da G. UBERTIS, G.P. VOENA), Milano, 2005, p. 41; G. CANSACCHI, *Assistenza giudiziaria internazionale*, in *Novissimo Digesto Italiano*, vol. I, Torino, 1964, p. 1408 ss.; G. DIOTALLEVI, *La c.d. “concelebrazione” delle rogatorie e gli atti diretti di giurisdizione all'estero*, in *Cass. pen.*, 3, 1998, p. 916; G. DI CHIARA, *Rapporti giurisdizionali con autorità straniere*, in *Enc. Dir.*, Agg. II, Milano, 1998, p. 893; I. IAI, *Rogatoria eseguita all'estero dall'autorità giurisdizionale dello Stato richiedente*, in *Giur. It.*, 7, 2000, p. 1471; I. CAMINITI, *L’effettiva portata del principio locus regit actum*, in *Giur. It.*, 10, 2002, p. 1919 ss.; D. CARCANO, *Principi generali della disciplina*, in AA.VV., *Rogatorie penali e cooperazione*

Sulla base di tale principio, lo Stato interessato ad acquisire un elemento di prova deve rivolgere una richiesta allo Stato in cui la fonte di prova è situata. Tale richiesta non va eseguita automaticamente, ma è sottoposta ad un vaglio preventivo da parte degli organi governativi e giudiziari dello Stato richiedente e dello Stato richiesto. La richiesta, se ritenuta ammissibile, viene eseguita secondo la *lex loci*, ossia seguendo le regole probatorie vigenti nello Stato in cui si trova la fonte di prova³⁷⁶.

Più semplicemente, la *lex loci* è la legge dell'ordinamento giuridico del Paese dove si compie l'atto, che indica le modalità e la disciplina per lo svolgimento di esso. La validità va valutata alla stregua delle regole dell'ordinamento giuridico del Paese richiesto, e non dello Stato richiedente l'assistenza.

Tale procedimento segue, inoltre, lo schema della richiesta. Essa si avvia con una richiesta di uno Stato (detto *richiedente*) a un altro Stato (detto *richiesto*). Quest'ultimo compie una valutazione caso per caso e può non dare seguito alle richieste. Con tale procedimento, lo Stato richiesto ha teoricamente una illimitata possibilità di rifiuto e, in caso di accoglimento, un'ampia discrezionalità nella scelta delle modalità di esecuzione della richiesta.

Il c.d. "metodo intergovernativo" prevede un ruolo attivo esercitato dal potere esecutivo: la decisione finale in merito all'esecuzione dell'atto non è assunta da un magistrato, ma da un organo politico – segnatamente dal governo –, in particolare, in Italia, dal Ministro della giustizia.

Siccome l'attività è compiuta sul territorio dello Stato richiesto, il modello appare coerente. Però comporta una serie di "effetti collaterali" tali da non renderlo efficiente e idoneo a soddisfare né le esigenze a causa negativa della cooperazione giudiziaria come la lotta alla criminalità transnazionale nel mondo contemporaneo, né le esigenze a causa positiva come il rispetto delle garanzie in capo all'indagato/imputato per via dei numerosi filtri a cui sono sottoposte le richieste di acquisizione probatoria.

Si pensi, ad esempio, al controllo governativo: un simile filtro rallenta l'intera attività istruttoria e comporta l'esercizio di un potere dai controlli sfumati e molto spesso non censurabile. Infatti, le decisioni assunte dall'autorità sovente non possono essere neppure motivate, affinché si eviti la diffusione di informazioni potenzialmente nocive per la sicurezza dei singoli Stati³⁷⁷.

Tale modello teorico ha bisogno ineluttabilmente di temperamenti finalizzati ad incrementare l'efficacia delle operazioni relative alla raccolta degli elementi di prova, perché in concreto l'applicazione non risulterebbe foriera di risultati apprezzabili. Un correttivo, ritenuto meramente fittizio da parte della dottrina perché sembra introdurre solo una deroga apparente alla *lex loci*³⁷⁸, sarebbe quello indicato all'art. 4 della Convenzione europea sulla mutua assistenza giudiziaria penale. Secondo tale articolo, «se la Parte richiedente ne fa domanda espressa, la Parte richiesta l'informerà della data e del luogo d'esecuzione della commissione rogatoria. Le autorità e le persone in causa potranno assistere all'esecuzione se la Parte richiesta vi acconsente».

Simile soluzione sembra ipotizzabile solo per quegli Stati che fanno parte del Consiglio d'Europa e che hanno ratificato la Convenzione. Infatti, tale regola non può

giudiziaria internazionale (a cura di E. CALVARESE, G. LA GRECA, M.R. MARCHETTI), Torino, 2003, p. 117 ss.; A. GAITO, *Dei rapporti giurisdizionali con autorità straniera*, Padova, 1985.

³⁷⁶ Così, M. DANIELE, *Ricerca e formazione della prova – Profili generali*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 458 ss.

³⁷⁷ Cfr., M. DANIELE, *Ricerca e formazione della prova – Profili generali*, cit., p. 459 ss.

³⁷⁸ Il riferimento è a E. ANODINA, *Cooperazione-integrazione penale nell'Unione europea*, in *Cass. pen.*, 10, 2001, p. 2898.

essere ritenuta principio universalmente riconosciuto di diritto internazionale. Ne consegue, quindi, che l'applicazione dell'art. 4 è sottoposto alla ratifica della Convenzione europea sulla mutua assistenza giudiziaria penale da parte del singolo Stato.

Tutte le deroghe al principio in esame sono dei semplici correttivi apposti alla regola generale, e come tali sono subordinate a una previsione esplicita all'interno della relativa Convenzione, bilaterale o multilaterale che sia, previa valutazione della loro compatibilità con i principi del proprio ordinamento da parte degli Stati stipulanti l'accordo³⁷⁹.

È per queste ragioni che, sebbene tale principio sia stato a lungo applicato da parte della quasi totalità degli ordinamenti statuali, si assiste oggi a un progressivo abbandono di tale modello tradizionale.

Gli Stati hanno raggiunto la consapevolezza che gli obiettivi delle rogatorie, e più in generale di tutti gli strumenti basati sinora sulla mutua assistenza, rischiavano di venire frustrati da una attività che, per le modalità di esecuzione, poteva condurre a un risultato inutilizzabile per lo Stato richiedente³⁸⁰.

Inoltre, rilevante dottrina osserva che l'abbandono del principio è dovuto anche ad una evoluzione dei sistemi processuali moderni in senso accusatorio, tanto da non poterlo più ritenere un principio generale internazionale³⁸¹.

Ed allora, a causa dei molteplici inconvenienti del principio della mutua assistenza, l'Unione europea ha individuato un principio più moderno, che presuppone un alto livello di integrazione dei sistemi processuali degli Stati, sul quale regolare i rapporti tra gli Stati membri nei casi di cooperazione giudiziaria in materia penale: il mutuo riconoscimento.

6. Il principio cardine della cooperazione giudiziaria tra Stati membri dell'Unione europea: il mutuo riconoscimento

Il mutuo riconoscimento è il principio strutturale³⁸² secondo cui le decisioni dei giudici penali o di altre autorità assimilate di uno Stato membro dell'Unione europea

³⁷⁹ Di tale avviso, C. VALENTINI, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Padova, 1998, p.187, spec. nota 17; M.R. MARCHETTI, *L'assistenza giudiziaria internazionale*, in AA.VV., *Trattato di procedura penale* (diretto da G. UBERTIS, G.P. VOENA), Milano, 2005, p. 45.

³⁸⁰ In realtà la normativa pattizia basata sul principio del *locus regit actum* è ormai scarsa e risalente nel tempo. Tra le tante convenzioni si ricordano, a titolo esemplificativo, la Convenzione con il Costa Rica firmata a Roma il 6 maggio 1873, la Convenzione con Cuba firmata a L'Avana il 4 ottobre 1928, il Trattato con il Venezuela firmato a Caracas il 23 agosto 1930 e la Convenzione con il Libano firmata a Beirut il 10 luglio 1970. È interessante rilevare come anche il codice di procedura penale italiano del 1930 si rifacesse a tale principio, laddove all'art. 658, comma 4, stabiliva «In ogni caso per il compimento degli atti richiesti si osservano le norme stabilite in questo codice». Le Convenzioni individuate, insieme ad altre, sono citate da M. PISANI, F. MOSCONI, *Codice delle Convenzioni di estradizione e di assistenza giudiziaria in materia penale*, Milano, 2003. Per un recente aggiornamento sui trattati in tema di assistenza giudiziaria e procedimento estradizionale, si vedano le tabelle B) e C) allegate in L. KALB, *Codice di procedura penale. Coordinato con le norme complementari*, Milano, 2021, p. 1665 ss.

³⁸¹ L'opinione è di E.N. LA ROCCA, *Le regole di esclusione della prova nel processo penale*, Roma, 2013, p. 180 ss. Sul tema si veda anche G. DARAIO, *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), IV, *Impugnazioni. Esecuzione penale. Rapporti con le autorità straniere* (a cura di L. KALB), Torino, 2015, p.1071.

³⁸² La dottrina maggioritaria qualifica il mutuo riconoscimento come principio generale dell'Unione europea, ritenendolo un principio strutturale avente una genesi di natura economica, ma dalle implicazioni squisitamente giuridiche. Sul punto, V. HATZOPOULOS, *Le principe communautaire d'équivalence et de reconnaissance mutuelle dans la libre prestation de services*, Athènes-Bruxelles, 1999, p. 111 ss.; F.

devono essere riconosciute ed eseguite allo stesso modo delle proprie dai giudici o dalle autorità degli altri Stati membri³⁸³.

TORIELLO, *I principi generali del diritto comunitario*, Milano, 2000, p. 117; C. JANSSENS, *The Principle of Mutual Recognition in EU Law*, Oxford, 2013, *passim*. Contrariamente, altra parte della dottrina ritiene che il mutuo riconoscimento sia una tecnica giuridica. In tal senso, S. NICOLIN, *Il mutuo riconoscimento tra mercato interno e sussidiarietà*, Padova, 2005, p. 229. V., inoltre, Commission of the European Communities, *Completing the Internal Market. White Paper from the Commission to the European Council (Milan, 28-29 June 1985)*, Brussels 14 June 1985, COM (85) 310 final.

³⁸³ La definizione è di J.R. SPENCER, *Il principio del mutuo riconoscimento*, cit., p. 341. Sulla definizione, inoltre, G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), cit., p. 998, secondo il quale «il provvedimento giudiziario estero (anche se di carattere interlocutorio, come la misura cautelare coercitiva, personale o reale) deve poter essere considerato e trattato come quello corrispondente emesso nel proprio ordinamento, nel senso di attribuirgli - attraverso, appunto, un atto di mutuo, reciproco riconoscimento - effetti identici o almeno analoghi alle decisioni domestiche, indipendentemente dal suo contenuto». V., anche, A. GAITO, *Spazio penale europeo e cooperazione giudiziaria internazionale*, cit., p. 976. In tema di mutuo riconoscimento la dottrina è vastissima. Si segnala, *ex multis*, C. AMALFITANO, *Unione europea e principio del reciproco riconoscimento delle decisioni penali*, in AA.VV., *L'ordine europeo di protezione. La tutela delle vittime di reato come motore della cooperazione giudiziaria* (a cura di H. BELLUTA, M. CERESA GASTALDO), Torino, 2016, p. 21; I. ARMADA, *The European Investigation Order and the lack of European Standards for Gathering Evidence: Is a fundamental Rights-based Refusal the solution?*, in *New Journal of European Criminal Law*, 1, 2015, p. 8 ss.; I. BANTEKAS, *The principle of mutual recognition in EU Criminal law*, in *European Law Review*, 3, 2007, p. 365 ss.; V. COVOLO, *Mutual Recognition and Absolute Standards of Effective Judicial Protection*, in AA.VV., *Effective Defence Rights in Criminal Proceedings* (a cura di S. ALLEGREZZA, V. COVOLO), Milano, 2018, p. 133 ss.; M. DANIELE, *Ricerca e formazione della prova*, in AA.VV., *Manuale di procedura penale europea* (a cura di R. KOSTORIS), Milano, 2019, p. 458 ss.; C. JANSSENS, *The Principle of Mutual Recognition in EU Law*, cit., *passim*; L. KLIMEK, *Mutual recognition of Judicial Decisions in European Criminal Law*, Berlino, 2017; L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, AA.VV., *L'ordine europeo d'indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 9 ss.; O. MAZZA, *Il principio del mutuo riconoscimento, la mancata armonizzazione e il mito taumaturgico della giurisprudenza europea*, in ID., *Il garantismo al tempo del giusto processo*, Milano, 2011, p. 55 ss.; A. MANGIARACINA, sub Art. 696-bis c.p.p., in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 12 ss.; ID., *Principi generali del mutuo riconoscimento*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 861 ss.; G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 466 ss.; V. MITSILEGAS, *The Symbiotic Relationship Between Mutual Trust and Fundamental Rights in Europe's Area of Criminal Justice*, in *New Journal of European Criminal Law*, 6, 4, 2015, p. 457 ss.; ID., *The Constitutional Implications of Mutual Recognition in Criminal Matters in EU*, in *Common Market Law Review*, 5, 2006, p. 1277; H. NILSSON, *From classical judicial cooperation to mutual recognition*, in *International Review of Penal Law*, 1, 2006, p. 53 ss.; H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, in *New Journal of European Criminal Law*, 1, 2019, p. 44 ss.; F. SIRACUSANO, *Tra mutuo riconoscimento e armonizzazione preventiva: quali prospettive per la circolazione della prova dichiarativa nell'ambito dell'Unione europea?*, in *Arch. pen.*, 1, 2012, p. 1 ss.; P. SPAGNOLO, *La Nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, cit., p. 1290 ss.; W. VAN BALLEGOOGIIJ, P. BÅRD, *Mutual recognition and individual rights. Did the Court get it right?*, in *New Journal of European Criminal Law*, 4, 2016, p. 439 ss. Esprime il concetto in termini diversi, M. POELEMANS, *Bilan et perspectives du principe de reconnaissance mutuelle en matière pénale en France*, in AA.VV., *The Future of Mutual Recognition in Criminal Matters in the European Union* (a cura di G. VERNIMMEN, VAN TIGGELEN, L. SURANO, A. WEYEMBERGH), Bruxelles, 2009, p. 240 secondo il quale il mutuo riconoscimento in ambito penale sottende «l'idea di uno Spazio europeo in seno al quale anche le decisioni giudiziarie rese in uno Stato membro possono circolare liberamente, nel senso che vanno riconosciute ed eseguite in qualunque altro Stato membro».

Per decisioni giudiziarie si intendono non solo le pronunce definitive ma anche i provvedimenti interlocutori, come gli atti coercitivi ad efficacia personale e reale³⁸⁴.

Con la Comunicazione della Commissione al Consiglio e al Parlamento europeo sul “riconoscimento reciproco delle decisioni definitive in materia penale” l’Unione europea, in generale, considera che «il riconoscimento reciproco sia un principio basato sull’idea che, nonostante un altro Stato possa non trattare una specifica questione in maniera uguale o simile a quella dello Stato stesso, la decisione adottata sarà tale da essere accettata come equivalente alla decisione che avrebbe adottato lo Stato interessato. La reciproca fiducia, non solo nell’adeguatezza della normativa dei propri partner, bensì anche nella corretta applicazione di tale normativa, è un fattore importante del riconoscimento reciproco. Sulla base di tale idea d’equivalenza e della fiducia reciproca, le conclusioni alle quali è giunto un altro Stato membro possono avere effetto sulla sfera d’influenza giuridica dello Stato membro interessato.

Di conseguenza, una decisione adottata da un’autorità in uno Stato membro potrebbe essere accettata in quanto tale in un altro Stato, anche nell’ipotesi in cui ivi non esista un’autorità analoga, o in grado di adottare tali decisioni, oppure nel caso in cui tale autorità avesse adottato una decisione totalmente differente in un caso compatibile. Riconoscere una decisione estera in materia penale significa attribuire a tale decisione effetti al di fuori dello Stato in cui è stata adottata, sia attribuendole gli effetti giuridici stabiliti dal diritto penale dello Stato estero, sia tenendone conto affinché espliciti gli effetti stabiliti dal diritto penale dello Stato che ha riconosciuto tale decisione. Il principio del riconoscimento reciproco procede spesso, ma non sempre, di pari passo con un determinato grado di armonizzazione dell’attività degli Stati membri, che spesso consente, in effetti, di accettare più facilmente i risultati raggiunti in un altro Stato. D’altro canto, il riconoscimento reciproco può in certa misura rendere inutile tale armonizzazione»³⁸⁵.

Come già osservato, alla base del mutuo riconoscimento in ambito penale vi è la formazione di uno spazio giudiziario europeo nel quale possono circolare liberamente anche le decisioni giudiziarie di uno Stato membro, affinché queste siano riconosciute ed eseguite in qualunque Stato dell’Unione europea³⁸⁶.

I presupposti su cui si fonda sono la fiducia reciproca nell’adeguatezza delle norme applicate in altri Stati membri; la fiducia reciproca nella corretta applicazione di queste norme negli altri Stati membri da parte dei tribunali e di altri organi di esecuzione della legge; e di conseguenza, l’accettazione dei risultati ottenuti nell’altro Stato membro sulla base delle sue leggi e dei suoi regolamenti applicati dai suoi tribunali e da altri organi di esecuzione della legge senza che il risultato sia verificato rispetto alle leggi e ai regolamenti nazionali³⁸⁷.

Per l’attuazione del principio è necessario un livello di integrazione dei sistemi processuali degli Stati più alto rispetto a quello dell’assistenza giudiziaria; una diretta cooperazione tra le autorità giudiziarie; una reciproca fiducia tra gli Stati, i quali riconoscono come valide le regole probatorie degli altri Stati, affinché possano liberamente circolare i provvedimenti emessi. Così facendo, all’interno del proprio

³⁸⁴ Così G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), cit., p. 514.

³⁸⁵ Cfr., COM (2000) 495 def., del 26 luglio 2000.

³⁸⁶ Così, G. VERNIMMEN, VAN TIGGELEN, L. SURANO, A. WEYEMBERGH (eds.), *The future of mutual recognition in criminal matters in the European Union*, Bruxelles, 2009.

³⁸⁷ Così, H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, cit., p. 46.

ordinamento è possibile recepire incondizionatamente, riconoscere e dare esecuzione alle decisioni di un giudice penale di un altro Stato, utilizzando formalità minime e potendo addurre limitati motivi di diniego³⁸⁸.

Ulteriore aspetto di semplificazione rispetto all'assistenza giudiziaria penale è l'assenza del filtro politico. Si crea così una procedura semplificata che stabilisce una linea comunicativa diretta tra le autorità giudiziarie, abbattendo in tal modo i tempi ed i costi relativi all'espletamento delle attività – in particolare, probatorie – nonché eliminando tutti gli ostacoli che sostanzialmente impediscono una rapida esecuzione dell'atto.

Il principio diventa, allora, strumento cardine della cooperazione giudiziaria, pregno di caratteristiche rivoluzionarie: esso garantisce, in netta contrapposizione al principio della mutua assistenza, una sensibile riduzione dei tempi delle procedure; un abbattimento dei costi; l'eliminazione di quella sovrastruttura rappresentata dal metodo intergovernativo e, quindi, dal filtro politico; l'eliminazione del principio del *locus regit actum* sostituito dal concetto di emissione/esecuzione; l'adozione della *lex fori* secondo cui l'atto verrà esperito seguendo le regole dello Stato che ha emesso l'ordine; la sostituzione dell'arrugginito schema della richiesta con lo schema dell'ordine basato su un modulo *standard*; la relativa impossibilità di rifiutare l'ordine; una procedura di controllo prevalentemente formale, meno rigida, dei requisiti estrinseci del provvedimento da eseguire e, più in generale, attività basate sui principi di semplicità, rapidità, immediatezza delle informazioni e delle procedure sia di trasferimento sia di esecuzione dei provvedimenti giudiziari.

Da ciò si ricavano i tre elementi attorno ai quali ruota il principio del mutuo riconoscimento: equivalenza, mutua fiducia ed extraterritorialità³⁸⁹.

La dottrina è solita suddividere il principio di mutuo riconoscimento in attivo e passivo³⁹⁰.

Per mutuo riconoscimento in senso passivo si intende l'obbligo, per il giudice penale di uno Stato membro, di attribuire alla decisione emessa da un altro ordinamento giuridico statale, facente parte dell'Unione europea, gli stessi effetti giuridici che sarebbero attribuiti a una decisione che provenga da un'autorità giudiziaria del proprio ordinamento.

In senso attivo si fa riferimento all'obbligo in capo ai giudici di uno Stato membro di emanare tutti i provvedimenti necessari per l'esecuzione, oltre a riconoscere come validi i provvedimenti e le decisioni dei giudici e delle autorità assimilate degli altri Stati membri.

³⁸⁸ In tal senso, si veda V. MITSILEGAS, *EU Criminal Law*, Oxford, 2009; A. PASQUERO, *Mutuo riconoscimento delle decisioni penali: prove di federalismo*, Milano, 2007; N. PARISI, *Riconoscimento reciproco delle decisioni giudiziarie penali, confiance mutuelle, e armonizzazione delle garanzie procedurali negli Stati membri dell'Unione europea*, in AA.VV., *Scritti in onore di Ugo Draetta*, (a cura di N. PARISI, M. FUMAGALLI MERAVIGLIA, D. RINOLDI, A. SANTINI), Napoli, 2011, p. 503 ss.; I. BANTEKAS, *The principle of mutual recognition in EU criminal law*, in *European Law Review*, 3, 2007, p. 365 ss.

³⁸⁹ In tal senso, I. ARMADA, A. WEYEMBERGH, *The mutual recognition principle and EU Criminal law*, in AA.VV., *The European Union as an Area of Freedom, Security and Justice* (a cura di M. FLETCHER, E. HERLIN-KARNELL, C. MATERA), London, 2017, p. 116.

³⁹⁰ Cfr. J. R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 314 ss.; V., anche, S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007, p. 691 ss.; A. GAITO, *Spazio penale europeo e cooperazione giudiziaria internazionale*, cit., p. 976.

Ad esempio, se un giudice spagnolo emette un mandato di arresto europeo nei confronti di una persona che in quel momento sia in Belgio, il giudice belga, se richiesto, dovrà eseguire il mandato spagnolo, seguendo la relativa procedura prevista per l'attuazione di tale strumento, fino all'arresto e al trasferimento in Spagna dell'arrestato, disponendo tutti i provvedimenti necessari.

La portata innovativa del principio è data dalla forte riduzione dei tempi per l'esecuzione della relativa procedura e dalla fluidificazione dei rapporti tra gli Stati membri, dovuta all'eliminazione di qualsiasi forma di filtro politico, in modo da consentire una lotta più efficace ed efficiente alla criminalità organizzata transnazionale, in un'ottica di massimizzazione dei risultati.

Fu questo il principale obiettivo che si pose il Consiglio di Tampere del 1999³⁹¹, durante il quale, rifacendosi a una proposta ufficiale del Consiglio europeo di Cardiff tenutosi l'anno precedente, venne individuato un programma³⁹² che rendesse la cooperazione giudiziaria più incisiva attraverso un processo di armonizzazione tra gli ordinamenti dei Paesi membri, secondo la strategia del “doppio binario” e individuando nel principio di mutuo riconoscimento il principio cardine, la “pietra angolare”³⁹³ della cooperazione.

³⁹¹ Per un approfondimento utile si legga a L. SALAZAR, *La costruzione di uno Spazio di libertà, sicurezza e giustizia dopo il Consiglio europeo di Tampere*, cit., p. 1114 ss.; P. BILANCIA, *Lo spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria*, in AA.VV., *Alle frontiere del diritto costituzionale: scritti in onore Valerio Onida* (a cura di M. D'AMICO, B. RANDAZZO), Milano, 2011, p. 197 ss.

³⁹² Si veda il Programma di misure per l'attuazione del principio del mutuo riconoscimento delle decisioni penali, in GUCE C 12 del 15 gennaio 2001 e le Conclusioni della Presidenza – Summit europeo di Tampere, del 15 e 16 novembre 1999, SN 200/99, punto 33, ove si afferma che «il rafforzamento del reciproco riconoscimento delle decisioni giudiziarie e delle sentenze ed il necessario ravvicinamento delle legislazioni faciliterebbero la cooperazione tra le autorità, come pure la tutela giudiziaria dei diritti dei singoli. Il Consiglio europeo approva il principio del reciproco riconoscimento che, a suo parere, dovrebbe diventare il fondamento della cooperazione giudiziaria nell'Unione, tanto in materia civile quanto in materia penale. Il principio dovrebbe applicarsi sia alle sentenze sia alle altre decisioni delle autorità giudiziarie».

³⁹³ Il principio del mutuo riconoscimento, altrimenti detto del riconoscimento reciproco, non era una vera e propria novità. In passato, era già utilizzato in numerosi Stati federali, in particolare nei sistemi di *common law*, anche nel settore della giustizia penale. Due sono gli esempi più rilevanti: Stati Uniti d'America e Regno Unito.

L'art. IV, §1 della Costituzione americana individua nel principio di mutuo riconoscimento, un sistema per regolare i rapporti tra gli Stati federati, i c.d. *Sister States*. L'articolo recita: «In ogni Stato saranno attribuiti piena fiducia e pieno credito agli atti, ai documenti pubblici e ai procedimenti giudiziari degli altri Stati. Il Congresso potrà, mediante leggi generali, prescrivere il modo in cui la validità di tali atti, documenti e procedimenti debba essere determinata e i suoi effetti», individuando, così, la c.d. clausola *full faith and credit*. In questo modo, si consente ai provvedimenti giudiziari delle autorità penali nazionali di circolare in uno spazio unico. Inoltre, l'art. IV, §2 disciplina l'extradizione interstatale su richiesta dell'organo esecutivo, nel caso in cui l'accusato sia fuggito da uno Stato.

Un sistema simile vige anche nei rapporti interordinamentali del Regno Unito, composto da tre sistemi giuridici e da tre sistemi di giustizia penale tra loro distinti e differenti: Inghilterra e Galles, Scozia, Irlanda del Nord. Le decisioni dei giudici penali appartenenti a uno di questi tre sistemi sono automaticamente riconosciute dai giudici che appartengono alle altre. Forte dei buoni risultati apportati nell'ordinamento inglese, il Presidente inglese Jack Straw, durante il Consiglio di Cardiff del 15 e 16 giugno 1998, propose l'applicazione di questo principio anche all'interno dell'Unione europea, quale “pietra angolare” o “regola aurea”. In particolare, al punto 39 delle conclusioni si afferma che: «il Consiglio europeo sottolinea l'importanza di una efficace cooperazione giudiziaria nella lotta contro la criminalità transnazionale. Esso riconosce che occorre potenziare la capacità dei sistemi giuridici nazionali di operare in stretto contatto e chiede al Consiglio di determinare in quale misura si debba estendere il riconoscimento reciproco delle decisioni dei rispettivi tribunali». Con il Consiglio di Tampere, si affermò che il mutuo riconoscimento

Il Consiglio europeo di Cardiff prima e il Consiglio di Tampere poi gettarono delle basi effettive per l'applicazione dell'innovativo principio del mutuo riconoscimento, principio tra l'altro non del tutto sconosciuto né dall'Unione europea né dagli ordinamenti extra – europei³⁹⁴: si pensi, ad esempio, alla Convenzione di Bruxelles del 1968, o all'art.

doveva diventare il fondamento della cooperazione giudiziaria tanto in materia civile, quanto in materia penale, in seno all'Unione. Il Consiglio europeo concluse espressamente che tale principio doveva altresì applicarsi alle sentenze e alle altre decisioni delle autorità giudiziarie (paragrafi da 33 a 37 delle conclusioni). In realtà, il principio era già stato ampiamente sperimentato con ottimi risultati nei settori della libera circolazione delle merci. La sua origine si deve alla sentenza della Corte di giustizia, 20 febbraio 1979, *Rewe Zentral AG c. Bundesmonopolverwaltung Fuer Branntwein*, causa C-120/78, più nota come “*Cassis de Dijon*”, relativa a un caso di libera circolazione di un liquore francese. Secondo quanto stabilito con tale sentenza, uno Stato membro non può ostacolare la circolazione nel proprio territorio nazionale di merce prodotta secondo gli *standard* dello Stato membro di produzione, sul presupposto che all'interno dello Stato membro lo *standard* è diverso. Sulle origini del principio del mutuo riconoscimento e sulla espansione nel settore della cooperazione giudiziaria in materia penale, A. DAMATO, P. DE PASQUALE, N. PARISI, *Argomenti di diritto penale europeo*, II ed., Torino, 2014, p. XXI ss.; G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in *Cass. pen.*, 1, 2006, p. 265B ss.; B. PIATTOLI, *Cooperazione giudiziaria e pubblico ministero europeo*, Milano, 2002, p. 94 ss.; A. PASQUERO, *Mutuo riconoscimento delle decisioni penali: prove di federalismo*, Milano, 2007, p. 58; L. SALAZAR, *La lotta alla criminalità dell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il Programma dell'Aia*, cit., p. 3512 ss.; J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 341 ss.; F. SPIEZIA, *La cooperazione giudiziaria internazionale e lo spazio di giustizia europeo*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), cit., p. 844 ss. Per l'applicazione del principio in materia cautelare, v., D. CIMADOMO, *Reciproco riconoscimento e “misure alternative” alla detenzione cautelare*, in AA.VV., *Cooperazione giudiziaria: le novità del recepimento delle fonti sovranazionali. Estratto* (a cura di L. KALB), in *Dir. pen. e proc.*, 8/9, 2016, p. 1015 ss. Sull'applicazione del principio del mutuo riconoscimento nelle decisioni di confisca, D. CIMADOMO, *Commento agli artt. 1-9 d. legisl. 7 agosto 2015, n. 137 (Attuazione della decisione quadro 2006/783/GAI relativa all'applicazione del principio del reciproco riconoscimento delle decisioni di confisca)*, in AA.VV., *Commentario breve al Codice antimafia e alle altre procedure di prevenzione* (a cura di G. SPANGHER, A. MARANDOLA), Milano, 2019, p. 445 ss.; L. KALB, *Commento agli artt. 10-17 d. legisl. 7 agosto 2015, n. 137 (Attuazione della decisione quadro 2006/783/GAI relativa all'applicazione del principio del reciproco riconoscimento delle decisioni di confisca)*, in AA.VV., *Commentario breve al Codice antimafia e alle altre procedure di prevenzione* (a cura di G. SPANGHER, A. MARANDOLA), Milano, 2019, p. 458 ss. In tema di mutuo riconoscimento nelle decisioni di confisca, v. inoltre le osservazioni formulate in M. ARLEO, *Commento a Corte cost., 8 novembre 2007 – 21 febbraio 2018, n. 33*, in AA.VV., *Corte costituzionale e sistema processuale penale. L'elaborazione giurisprudenziale del 2018* (a cura di D. CIMADOMO, G. DALIA), Milano, 2019, p. 1 ss.

³⁹⁴ Un eclatante esempio di applicazione del principio del mutuo riconoscimento – vicino ad un modello puro – è relativo all'assistenza giudiziaria tra Paesi nordici, già attuata decenni prima di Tampere e del mandato d'arresto europeo (MAE). Alla fine degli anni '50 e all'inizio degli anni '60, Danimarca, Finlandia, Islanda, Norvegia e Svezia stabilirono un sistema separato di estradizione “intra-nordica”, non basato su alcun trattato tra quei Paesi. Non c'era alcun obbligo di estradare: il sistema si basava esclusivamente sulla disponibilità reciproca di cooperare a livello pratico e sulla possibilità concreta di farlo. La base era una legislazione nazionale essenzialmente uniforme sull'extradizione. Di conseguenza, con un minimo di formalità, è stato ottenuto un sistema di estradizione più efficace ed efficiente basato sulla fiducia reciproca. Non c'era nemmeno il requisito della doppia incriminabilità e la soglia della pena per considerare un reato estradabile era molto bassa: qualsiasi atto, che non fosse solo punibile con una multa, era sufficiente per dare luogo all'extradizione. L'assenza di qualsiasi obbligo di estradizione del sistema si è rivelata estremamente flessibile e ha consentito, ad esempio, la non estradizione per mancanza di proporzionalità. Oggi il sistema è stato sostituito dal *Nordic Arrest Warrant*. Cfr., the Swedish Act No. 254, adottato il 5 giugno 1959; the Danish Act No. 27, adottato il 3 febbraio 1960; the Finnish Act No. 270, adottato il 3 giugno 1960; the Norwegian Act No. 1, adottato il 3 Marzo 1961; the Icelandic Act No. 7, adottato il 14 Marzo 1962. In dottrina, P. ASP, *Nordic Judicial Co-operation in Criminal Matters*, Uppsala, 1998; G. MATHISEN, *Nordic Cooperation and the European Arrest Warrant: Intra-Nordic Extradition, the Nordic*

IV, §1 della Costituzione degli Stati Uniti d'America, o ancora al sistema di mutuo riconoscimento adottato dal Regno Unito per regolare i propri rapporti interordinamentali³⁹⁵.

L'affermazione del principio nel panorama internazionale è però dovuta al lungo e duro lavoro compiuto dall'Unione europea, attenta allo sviluppo di un sistema di cooperazione giudiziaria moderno, evoluto ed al passo con le nuove sfide poste dai progressi sociali e tecnologici.

Ed infatti, nel 2001 la Commissione e il Consiglio dei Ministri per la Giustizia e gli affari interni, a seguito del vertice europeo di Laeken, emanarono un programma necessario per l'attuazione del principio del mutuo riconoscimento, destinato a concretizzare, tra le altre cose, il mandato di arresto europeo (MAE) e l'ordine europeo di indagine penale (OEI), nonché tutta una serie di strumenti basati su tale principio. Sovente si tratta di strumenti ibridi, nati dalla fusione di alcuni aspetti del mutuo riconoscimento con le classiche caratteristiche di altri principi³⁹⁶.

Arrest Warrant and Beyond, in *Nordic Journal of International Law*, 1, 2010, p. 1 ss. Per il *Nordic Arrest Warrant* si rinvia alla Convention on Surrender for Criminal Acts between the Nordic Countries (*Nordic Arrest Warrant*) [*Konvention om overgivelse for straffbare forhold mellem de nordiske lande (Nordisk arrestordre)*] del 15 dicembre 2005; in dottrina, A. STRANDBAKKEN, *The Nordic Answer to the European Arrest Warrant: The Nordic Arrest Warrant*, in *Eucrim*, 3-4, 2007, p. 138 ss. Più in generale, v. H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, cit., p. 48 ss.

³⁹⁵ La Convenzione di Bruxelles sulla competenza giurisdizionale e l'esecuzione delle decisioni in materia civile e commerciale venne adottata dalla Comunità Economica Europea il 27 settembre 1968. Tale Convenzione istituì un sistema nei rapporti tra gli Stati membri della allora Comunità economica europea secondo il quale sia il riconoscimento che l'esecuzione delle decisioni assunte in materia civile e commerciale erano automatici. La Convenzione è stata di fatto sostituita nel 2001 dal regolamento CE 44/2001 del Consiglio, vincolando di fatto tutti gli Stati membri dell'Unione europea.

³⁹⁶ Tra i vari strumenti basati sul principio si ricordano: la decisione quadro 2002/584/GAI del 13 giugno 2002 che ha istituito il mandato di arresto europeo in GUUE L-190/1 del 18 luglio 2002; la decisione quadro 2003/577/GAI del Consiglio del 22 luglio 2003, relativa all'esecuzione nell'Unione europea dei provvedimenti di blocco dei beni o di sequestro probatorio, in GUUE L-196/45 del 2 ottobre 2003; la decisione quadro 2005/214/GAI del Consiglio del 24 febbraio 2005, relativa all'applicazione del principio del reciproco riconoscimento alle sanzioni pecuniarie in GUUE L-76/16 del 22 marzo 2005; la decisione quadro 2006/783/GAI del Consiglio del 6 ottobre 2006, relativa all'applicazione del principio del reciproco riconoscimento delle decisioni di confisca in GUUE L-382/59 del 24 novembre 2006; la decisione quadro 2008/299/GAI relativa alle decisioni pronunciate *in absentia*; la decisione quadro 2008/675/GAI del Consiglio del 24 luglio 2008, relativa alla considerazione delle decisioni di condanna tra gli Stati membri dell'Unione europea in occasione di un nuovo procedimento penale in GUUE L-220/32 del 15 agosto 2008; la decisione quadro 2008/947/GAI del Consiglio del 27 novembre 2008, relativa all'applicazione del principio del reciproco riconoscimento alle sentenze e alle decisioni di sospensione condizionale in vista della sorveglianza delle misure di sospensione condizionale e delle sanzioni sostitutive in GUUE L-337/102 del 16 dicembre 2008; la decisione quadro 2008/909/GAI del Consiglio del 27 novembre 2008 relativa all'applicazione del principio del reciproco riconoscimento alle sentenze penali che irrogano pene detentive o misure privative della libertà personale, ai fini della loro esecuzione nell'Unione europea in GUUE L-327/27 del 5 dicembre 2008; la decisione quadro 2008/978/GAI del Consiglio del 18 dicembre 2008 sul mandato di ricerca delle prove, diretto all'acquisizione di oggetti, documenti, e dati da utilizzare nei procedimenti penali in GUUE L-350/72 del 30 dicembre 2008; la decisione quadro 2009/829/GAI del Consiglio del 23 novembre 2009 sull'applicazione tra gli Stati membri dell'Unione europea del principio del reciproco riconoscimento alle decisioni sulle misure alternative alla detenzione cautelare, in GUUE L-294/90 dell'11 novembre 2009; la decisione quadro 2009/948/GAI relativa alla prevenzione e risoluzione dei conflitti di giurisdizione; la dir. 2011/99/UE del Parlamento europeo del 13 dicembre 2011 sull'ordine di protezione europeo in GUUE L-38/2 del 21 dicembre 2011; la dir. 2014/41/UE del Parlamento europeo e del Consiglio relativa all'ordine europeo di indagine penale in GUUE L-130/1 del 15 maggio 2014. Sul reciproco riconoscimento alle sanzioni pecuniarie, previsto con decisione quadro 2005/214/GAI, A. MARANDOLA, *Reciproco riconoscimento alle decisioni sulle sanzioni pecuniarie (d.lg. n. 37/2016)*, in

Confermata la sua importanza sia con il Programma dell'Aja del novembre 2004³⁹⁷ che con il Programma di Stoccolma del dicembre 2009³⁹⁸, il principio riceve la propria definitiva consacrazione attraverso l'espressa previsione nel Trattato di Lisbona. Infatti nella parte terza, titolo V relativo allo Spazio di libertà, sicurezza e giustizia, al capo 4 relativo alla disciplina della cooperazione giudiziaria in materia penale, l'art. 67, par.3 TFUE sancisce che: «L'Unione si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali», mentre al par. 4: «L'Unione facilita l'accesso alla giustizia, in particolare attraverso il principio di riconoscimento reciproco delle decisioni giudiziarie ed extragiudiziali in materia civile». Infine, l'art. 82 TFUE recita: «La cooperazione giudiziaria in materia penale nell'Unione è fondata sul principio di riconoscimento reciproco delle sentenze e delle decisioni giudiziarie».

Dunque, il principio del mutuo riconoscimento, per essere effettivo, deve fondarsi sul principio della fiducia reciproca tra gli ordinamenti giuridici, ispirati ai valori dello Stato democratico di diritto, informato al rispetto dei diritti umani.

AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 925 ss. Sull'attuazione della decisione quadro 2003/577/GAI in Italia, G. DARAIO, *L'attuazione della d.q. 577/2003 sul reciproco riconoscimento dei provvedimenti di sequestro o di confisca*, in *Dir. pen. e proc.*, 9, 2016, p. 1133 ss. In tema di applicazione del principio del reciproco riconoscimento alle sentenze penali che irrogano pene detentive o misure privative della libertà personale, ai fini della loro esecuzione nell'Unione europea prevista dalla decisione quadro 2008/909/GAI, A. MARANDOLA, *Reciproco riconoscimento alle sentenze penali che irrogano pene detentive o misure privative della libertà personale (d. lg. n. 161/2010)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 874 ss.; S. MONTALDO, *The Road Ahead: Proposals for Improving the Implementation of Framework Decision 2008/909/JHA*, in AA.VV., *The Transfer of Prisoners in the European Union Challenges and Prospects in the Implementation of Framework Decision 2008/909/JHA* (a cura di S. MONTALDO), The Hague, 2020, p. 141 ss.; ID., *Framework Decision 2008/909/JHA on the transfer of prisoners in the EU: Advances and challenges in light of the Italian experience*, in *The New Journal of European Criminal Law*, 1, 2020, p. 69 ss.; ID., *Framework Decision 2008/909/JHA and Fundamental Rights Concerns: In Search of Appropriate Remedies*, in AA.VV., *The Transfer of Prisoners in the European Union Challenges and Prospects in the Implementation of Framework Decision 2008/909/JHA* (a cura di S. Montaldo), The Hague, 2020, p. 37 ss.; A. ROSANÒ, *Framework Decision 2008/909/JHA in Context: Interplay with the European Arrest Warrant and (EU) Extradition Law*, in AA.VV., *The Transfer of Prisoners in the European Union Challenges and Prospects in the Implementation of Framework Decision 2008/909/JHA* (a cura di S. MONTALDO), The Hague, 2020, p. 79 ss. In merito alla decisione quadro 2008/947/GAI, F.P.C. IOVINO, *Effetti del reciproco riconoscimento per l'esecuzione delle misure di sospensione condizionale delle sanzioni sostitutive*, in *Dir. pen. e proc.*, 9, 2016, p. 1148 ss.; A. MARANDOLA, *Reciproco riconoscimento delle decisioni sulle misure alternative alla detenzione cautelare (d.lg. 36/2016)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 903 ss.; A. MARANDOLA, *Reciproco riconoscimento delle decisioni di sospensione condizionale in vista della sorveglianza delle misure di sospensione condizionale e delle sanzioni sostitutive (d.lg. n. 38/2016)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 945 ss.; S. MONTALDO, *The cross-border enforcement of probation measures and alternative sanctions in the EU: The poor application of Framework Decision 2008/947/JHA*, in *EU Law Enforcement*, 31 gennaio 2020, p. 1 ss., disponibile al link: <https://eulawenforcement.com/?p=7353>

³⁹⁷ Cfr. *The Hague Programme*, Bruxelles, Consiglio europeo, Presidency Conclusions, 4 e 5 novembre 2004, in GUCE C 53, 3 marzo 2005.

³⁹⁸ Cfr. *The Stockholm Programme*, Stoccolma, Consiglio europeo, Presidency Conclusion, 11 dicembre 2009, in GUCE C 115, 4 e 5 maggio 2010.

7. Il mutuo riconoscimento quale presupposto per la “libera circolazione” delle decisioni giudiziarie

L'utilità del principio di mutuo riconoscimento è apparsa evidente agli Stati membri nel momento in cui si è compreso come l'apertura dei mercati abbia generato un aumento della criminalità organizzata transnazionale. È necessario capire secondo quali circostanze il metodo proposto dal mutuo riconoscimento riesce a rispondere al meglio alle esigenze a causa negativa e a causa positiva.

Uno degli obiettivi dell'Unione europea è implementare ed accrescere la portata delle quattro libertà: la libera circolazione delle persone, dei mezzi, delle merci e dei capitali. A queste, come già osservato, se ne aggiunge una quinta non voluta, a carattere negativo: la libera circolazione della criminalità. L'obiettivo diventa, quindi, rispondere alla quinta libertà con strumenti specifici che, a differenza degli strumenti dell'assistenza giudiziaria, rendano più semplici e veloci le procedure.

Dinnanzi a tale situazione, l'Unione europea non poteva rimanere silente, né tantomeno poteva continuare ad affidarsi all'arrugginito modello basato sulla mutua assistenza. Pertanto, ha fatto ricorso al principio del mutuo riconoscimento, ritenuto particolarmente efficace nella lotta contro i crimini transfrontalieri e contro i nuovi crimini che, con il progresso scientifico e tecnologico, esordiscono prepotentemente sulla scena europea ed internazionale.

L'applicazione del principio del mutuo riconoscimento quale strumento di incentivazione della libera circolazione non era una assoluta novità per gli Stati membri. Esso era applicato già in tantissimi altri settori del diritto come l'ambito commerciale e ambientale. La difficoltà, però, stava nel giustificare la correlazione tra il principio e la libera circolazione.

Orbene, nella materia civile e commerciale, il collegamento tra libera circolazione e mutuo riconoscimento è evidente: appariva ovvio che, se l'obiettivo fosse attuare la libera circolazione delle persone, dei servizi, delle merci e dei capitali, di conseguenza si può consentire il libero commercio transfrontaliero mediante la garantita celerità dei traffici attraverso un riconoscimento automatico delle decisioni dei giudici civili in materia commerciale da parte di tutti i Paesi membri dell'Unione europea³⁹⁹.

Diversamente, invece, in ambito penale le “quattro libertà” non hanno reso pienamente evidente la necessità dell'applicazione di tale principio, perché, appunto, nate con caratteristiche di natura spiccatamente civilistica e commerciale. L'affermazione di esso in ambito penale è stata più complicata, in ragione della marcata difficoltà di giustificare l'implementazione del mutuo riconoscimento all'interno dell'ordinamento dell'Unione europea nello specifico settore penale.

Risultava però palese che l'aumento della criminalità transnazionale, la globalizzazione dei mercati e l'avvento di nuove forme di telecomunicazione e delle tecnologie informatiche richiedevano risposte serie e concrete dal punto di vista penale. Si aggiunga, inoltre, l'assoluta inefficienza dell'assistenza giudiziaria, ormai ridotta a una mera sovrastruttura non più in grado di rispondere alle nuove e specifiche esigenze del periodo.

³⁹⁹ Sul tema, *ex multis*, si veda G. STROZZI, *Diritto dell'Unione europea*, V ed., Torino, 2017; F. POCAR, *L'assistenza giudiziaria internazionale in materia civile*, Padova, 1967; U. DRAETTA, N. PARISI, *Elementi di diritto dell'Unione europea. Parte speciale*, IV ed., Milano, 2014.

Dunque, il tradizionale principio della mutua assistenza è in via di superamento, perché incentrato prevalentemente sulla dimensione nazionale del fenomeno criminale, a favore del più moderno e avanzato modello basato sul mutuo riconoscimento.

Si abbandona l'idea del rapporto bilaterale nell'interesse esclusivo dello Stato richiedente, proprio dell'assistenza giudiziaria, a favore di una collaborazione prestata da uno Stato a un altro Stato, basata su un interesse sia dello Stato emittente che dello Stato dell'esecuzione, per rispondere in modo deciso ed efficiente alla crescente dimensione sovranazionale e transnazionale della criminalità organizzata, ai *cross-border crimes*, ai reati finanziari, alla corruzione politica, al terrorismo internazionale e alle problematiche dei grandi traffici illeciti come droga, esseri umani, armi, rifiuti⁴⁰⁰, nonché alla prova elettronica, dalla spiccata natura potenzialmente sovranazionale.

Alla luce di tutto ciò, l'Unione europea, negli ultimi venti anni circa, si è mossa in una duplice direzione: da una parte si è dotata di strutture e organismi comuni in grado di agevolare e supportare le autorità nazionali nelle indagini e nei processi aventi carattere transnazionale, caratterizzati dal coinvolgimento delle autorità giudiziarie e di polizia di più Paesi; dall'altra, ha dato un serio impulso alla creazione di moderni strumenti di cooperazione, soprattutto per quanto riguarda la ricerca e la formazione transnazionale degli elementi di prova, ponendo in crisi il tradizionale metodo della rogatoria.

Con ciò, sembra potersi affermare che il principio del mutuo riconoscimento sia indubbiamente collegato alla libera circolazione anche nel contesto penale, in quanto è da ritenersi principio necessario per combattere le conseguenze indesiderate di essa con efficacia ed efficienza. Ed allora, come possono circolare liberamente tra gli Stati membri i mezzi, le persone, i servizi e i capitali, altrettanto deve avvenire per le decisioni del giudice, utili a combattere le nuove forme di criminalità. Nasce così la "libera circolazione delle decisioni giudiziarie" anche in ambito penalistico⁴⁰¹.

Ma che cosa si intende per "libera circolazione"? Come si giustifica il mutuo riconoscimento alla luce della "libera circolazione"? Ma soprattutto, qual è l'oggetto della libera circolazione nel settore penale?

La dottrina definisce la "libera circolazione" come «il movimento in senso geografico del trasferimento di un oggetto da un Paese ad un altro senza che l'esistenza di una frontiera possa bloccare il flusso»⁴⁰².

⁴⁰⁰ Per questa impostazione, cfr. G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), cit., p. 516; sul tema si veda anche M. PANEBIANCO, *L'approvazione parlamentare del mandato d'arresto europeo*, in AA.VV., *Mandato d'arresto europeo e garanzie della persona* (a cura di M. PEDRAZZI), Milano, 2004, p. 191 ss.

⁴⁰¹ Sul tema si legga J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 346 ss. L'autore osserva che il principio della libera circolazione delle decisioni giudiziarie è inoltre espresso al punto 6 del Preambolo del regolamento CE n. 44 del 2001 sul riconoscimento e l'esecuzione delle decisioni civili, dove si precisa che «per realizzare l'obiettivo della libera circolazione delle decisioni in materia civile e commerciale è necessario ed opportuno che le norme riguardanti la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni siano stabilite mediante un atto giuridico comunitario cogente e direttamente applicabile»; mentre al punto 10 si afferma che «in vista della libera circolazione delle sentenze, le decisioni emesse in uno Stato membro che sia soggetto al regolamento devono essere riconosciute ed eseguite in un altro Stato membro ugualmente soggetto al medesimo, anche se il debitore condannato sia domiciliato in uno Stato terzo».

⁴⁰² S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 700.

Si dà, quindi, l'idea del dinamismo dovuto al movimento di qualcosa in uno spazio – nel caso di specie nello “spazio giudiziario europeo” rispettoso del pluralismo degli ordinamenti che lo compongono – liberamente e senza che trovi dinnanzi a sé un ostacolo che possa bloccare la circolazione. Si tratta di un'entità libera di muoversi poiché in possesso di determinate caratteristiche, riconosciute da tutti i Paesi dell'Unione europea, che lo rendono idoneo allo spostamento.

In materia penale, per “libera circolazione” si intende la possibilità, per l'atto processuale, per la persona indagata, imputata o condannata, per la fonte o l'elemento probatorio e per l'oggetto di confisca, di essere trasferiti da un Paese all'altro, poiché legittimati da un provvedimento riconosciuto avente valore uguale o simile ad un atto interno corrispondente⁴⁰³.

Non è possibile ritenere sussistente un'analogia tra la libera circolazione delle merci, dei servizi, dei capitali e delle persone e la libera circolazione delle decisioni giudiziarie, poiché, mentre la libera circolazione delle merci garantisce una generale astensione dall'intervento diretto dei Paesi membri, la libera circolazione delle decisioni giudiziarie obbliga, invece, gli Stati membri a recepire ed eseguire gli atti giuridici che provengono da un altro Stato⁴⁰⁴.

Ad esempio, nell'Unione europea la libera circolazione di un bene edibile come il formaggio è garantita in virtù del fatto che, essendo prodotto in uno Stato membro nel rispetto degli *standard* sanitari e di etichettatura richiesti, gli altri Stati non potranno proporre azioni atte ad impedire la commercializzazione di esso su tutto il proprio territorio; *a contrario*, la libera circolazione delle decisioni giudiziarie non può essere garantita se non prevedendo come necessaria una ulteriore attività che i giudici o l'autorità giudiziaria debbano intraprendere per darvi esecuzione. Si ponga il caso del mandato di arresto europeo: una volta che il giudice di uno Stato membro ha emesso il provvedimento, le autorità giudiziarie degli altri Stati dovranno prendere tutte le misure idonee affinché il provvedimento venga eseguito, nel rispetto della relativa normativa che regola l'atto giuridico, e procedere, se il caso, all'arresto.

Proprio in tema di circolazione della prova si sono avute le maggiori difficoltà. Questo perché la prova è qualcosa di molto più complesso ed articolato rispetto ai beni commerciabili. Infatti, essa – intesa in senso ampio – affronta un lungo procedimento diviso in fasi che vanno dalla ricerca, all'ammissione, all'assunzione e, infine, alla valutazione, seguendo precise regole, diverse da un ordinamento all'altro⁴⁰⁵, o come preferisce altra dottrina, seguendo «una costruzione legale astratta»⁴⁰⁶, in grado di

⁴⁰³ In tal senso S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 701.

⁴⁰⁴ L'osservazione è di J. R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea*, (a cura di R.E. KOSTORIS), cit., p. 319.

⁴⁰⁵ Sul punto, parla di «fattispecie processuale complessa», L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, cit., p. 14.

⁴⁰⁶ L'espressione è di S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 710, la quale guarda all'elemento probatorio come risultato di una «fattispecie processuale astratta», legato agli ordinamenti in cui viene assunto.

incidere sull'utilizzabilità e/o sull'attendibilità del dato probatorio nello Stato di emissione, ossia lo Stato che ha richiesto l'atto⁴⁰⁷.

Ed è proprio qui che il principio del mutuo riconoscimento sprigiona tutta la propria potenza. Infatti, senza il mutuo riconoscimento, la libera circolazione delle decisioni giudiziarie non potrebbe essere effettiva poiché l'atto non potrebbe esser riconosciuto con semplicità come complementare ad un corrispondente atto del diritto interno, venendo a mancare tutta la relativa attività svolta per trasferire fisicamente l'atto giuridico in un altro Stato. Quindi, il mutuo riconoscimento è principio (e mezzo) necessario, ma non sufficiente, a garantire il risultato della libera circolazione, poiché assicura che al trasferimento dell'atto in un altro Stato segua il riconoscimento giuridico e l'esecuzione dell'atto stesso⁴⁰⁸.

Principio necessario, ma non sufficiente. Questo perché sembra comunque essenziale individuare un atto interno corrispondente all'atto estero e procedere a una comparazione ai fini della validità. Tale operazione, però, non è sempre agevole poiché rispetto del pluralismo degli ordinamenti vuol dire anche eterogeneità dei sistemi e degli atti da essi adottati: l'estrema difficoltà è rinvenire l'atto affine.

Si aggiungano, poi, le difficoltà di una corretta traduzione e definizione, nonché i fuorvianti *nomen iuris* spesso dati agli atti, i quali rendono il terreno di lavoro ancora più spinoso per l'operatore del diritto che si accinge a gestire e a districarsi nel complesso mondo della cooperazione giudiziaria, per arrivare a una triste conseguenza: il provvedimento o la decisione di un giudice efficace in uno Stato può risultare inefficace in un sistema giuridico diverso quando ad essi viene data esecuzione⁴⁰⁹.

⁴⁰⁷ In tal senso L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 14.

⁴⁰⁸ Sull'applicazione del principio del mutuo riconoscimento in materia penale, si veda S. GLESS, *Zum prinzip der gegenseitigen Anerkennung*, in *ZStW*, 2004, p. 353 ss.; in tema anche O. MAZZA, *Il garantismo al tempo del giusto processo*, Milano, 2008, p. 55 ss.; F. SIRACUSANO, *Tra mutuo riconoscimento e armonizzazione preventiva: quali prospettive per la circolazione della prova dichiarativa nell'ambito dell'U.E.?*, cit., p. 1 ss.

⁴⁰⁹ Sul punto si veda N. GALANTINI, *Una nuova dimensione per il ne bis in idem internazionale*, in *Cass. pen.*, 10, 2004, p. 3474 ss.; S. MANACORDA, *Il mandato di arresto europeo nella prospettiva sostanzial-penalistica: implicazioni teoriche e ricadute politico-criminali*, in *Riv. it. Dir. proc. Pen.*, 3, 2004, p. 789 ss.; R. BARATTA, *L'equivalenza delle normative nazionali ai sensi dell'art. 100B del Trattato CE*, in *Rivista di diritto europeo*, 1993, p. 727 ss.; S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 701. Interessante è poi il pensiero di J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea*, (a cura di R.E. KOSTORIS), cit., p. 347: l'autore arriva a tale assunto analizzando le Conclusioni della conferenza di Tampere relativa all'istituzione di uno strumento che assicuri la libera circolazione della prova nei procedimenti penali. Partendo dal presupposto che l'ammissibilità di un atto raccolto secondo le regole dello Stato estero – e quindi proveniente da altro Stato – nei procedimenti di uno Stato membro è automatica, osserva che è possibile compiere due interpretazioni: «secondo una interpretazione restrittiva, potrebbe significare solamente che se, ove siano rispettate le regole interne sulle modalità di assunzione della prova, la prova ottenuta vada ammessa nei procedimenti penali celebrati negli altri Stati membri, anche quando essi prevedano regole diverse in materia». Così interpretato, il principio della libera circolazione della prova risulterebbe vantaggioso, seppur con il rischio di una diminuzione delle garanzie date dallo Stato emittente qualora questo risulti più garantista rispetto allo Stato di esecuzione. In modo semplice: è possibile, ad esempio, che l'Italia chieda ad un altro Stato di eseguire una perquisizione. La perquisizione in Italia è un atto “a sorpresa” al quale il difensore ha facoltà di assistere senza un previo avviso datogli almeno ventiquattro ore prima del compimento dell'atto stesso. Analoga condizione, però, non è prevista nello Stato di esecuzione, il quale non prevede tale facoltà. Orbene, così inteso, lo Stato italiano non potrebbe rifiutare gli elementi

Allora, per l’acquisizione della prova non basta solo l’applicazione del mutuo riconoscimento e il rispetto della normativa prevista nello Stato di esecuzione, poiché «per circolare, la prova deve essere compatibile non soltanto con le norme del Paese in cui viene raccolta, ma anche con i principi del Paese in cui viene utilizzata ai fini decisori»⁴¹⁰.

Questo vuol dire che, affinché un atto giuridico – quale, ad esempio, un elemento probatorio – abbia efficacia e sia utilizzabile in uno Stato diverso da quello in cui è stato raccolto, non basta che venga trasferito in uno Stato membro e che rispetti i requisiti qualitativamente omogenei fissati in tutti gli Stati membri, ma occorrono, altresì, che vi siano norme minime relative all’ammissibilità e all’ utilizzabilità dei risultati probatori validi per tutti i procedimenti penali celebrati all’interno dell’Unione europea⁴¹¹.

Ne deriva, allora, che il compito diventa più semplice qualora sia portata avanti una preventiva opera di “armonizzazione” compiuta da tutti i Paesi membri dell’Unione europea. Sullo sfondo rimane, però, un elemento ormai apparentemente sbiadito, ma necessario ed utile per la sopravvivenza del principio del mutuo riconoscimento e per la sua applicazione: la fiducia reciproca tra gli Stati membri.

rinvenuti a seguito dell’esperimento dell’attività svolta, sul presupposto che la mera facoltà di assistere all’attività da parte del difensore sia prevista secondo le regole interne, ma esclusa dalle regole dello Stato di esecuzione. Tutto ciò, si badi bene, qualora il principio venga applicato “puramente”, senza alcun correttivo. Altra interpretazione, invece, più ampia, coinvolge il concetto di ammissibilità dell’elemento probatorio. In tal senso, il principio della “libera circolazione della prova” «potrebbe essere interpretato nel senso che qualunque prova legittimamente formata in uno Stato membro dovrebbe ritenersi automaticamente ammissibile in ogni altro Stato membro, anche quando essa sia vietata secondo le regole interne di quest’ultimo. Si pensi al principio che impone la testimonianza orale in certe materie. In base a una simile interpretazione, una dichiarazione scritta ottenuta legittimamente da un testimone nello Stato A, nel quale le dichiarazioni scritte sono generalmente ammissibili in sostituzione di una prova orale, dovrebbe essere riconosciuta a tutti gli effetti come prova nello Stato B, dove invece la prova orale è normalmente obbligatoria e le dichiarazioni testimoniali scritte sono in linea di principio vietate». In tal caso, l’ingiustizia che ne scaturirebbe dall’applicazione del principio della “libera circolazione della prova”, sarebbe del tutto evidente.

⁴¹⁰ Testualmente, E. AMODIO, *Diritto di difesa e diritto alla prova nello spazio giuriditario europeo*, in AA.VV., *Il difensore e il Pubblico Ministero europeo* (a cura di A. LANZI, F. RUGGIERI, L. CAMALDO), Padova, 2002, p. 107.

⁴¹¹ Tale soluzione era già ampiamente auspicata nel Libro Verde sulla ricerca delle prove in materia penale tra Stati Membri e sulla garanzia della loro ammissibilità, presentato l’11 novembre 2009, COM (2009) 624 definitivo, e ribadito nel Programma di Stoccolma – Un’Europa aperta e sicura al servizio e a tutela dei cittadini, in GUUE, C 115/12, 4 maggio 2010, secondo cui la soluzione più efficace per superare le difficoltà sinora esposte sembrava consistere nell’adozione di norme comuni per la raccolta delle prove in materia penale. Sul tema, si veda anche, L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in AA.VV., *L’ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 15.

8. La “fiducia reciproca” e il rispetto dei diritti fondamentali quali elementi necessari per il mutuo riconoscimento

La libera circolazione probatoria transnazionale⁴¹² non potrebbe essere perseguita se non si fondasse su una elevata fiducia reciproca⁴¹³ tra ordinamenti giuridici ispirati ai principi della democrazia e dello Stato di diritto, nonché al rispetto dei diritti umani.

⁴¹² Non bisogna confondere la circolazione probatoria transnazionale, col quale si fa riferimento a materiale probatorio di origine estera, con la c.d. circolazione probatoria interna che riguarda il trasferimento dei dati probatori tra procedimenti tutti in corso di svolgimento in Italia. La norma cardine è l'art. 238 c.p.p. che disciplina l'acquisizione di verbali di prova di altri procedimenti, civili e penali, subordinando l'acquisizione a precise condizioni che sono diversamente modulate a seconda che si tratti di mezzi di prova ovvero di atti di indagine e in questo secondo caso a seconda che si tratti di atti ripetibili o irripetibili. L'art. 238 c.p.p. recita: «1. È ammessa l'acquisizione di verbali di prove di altro procedimento penale, se si tratta di prove assunte nell'incidente probatorio o nel dibattimento. 2. È ammessa l'acquisizione di verbali di prove assunte in un giudizio civile definito con sentenza che abbia acquistato autorità di cosa giudicata. 2-bis. Nei casi previsti dai commi 1 e 2 i verbali di dichiarazioni possono essere utilizzati contro l'imputato soltanto se il suo difensore ha partecipato all'assunzione della prova o se nei suoi confronti fa stato la sentenza civile. 3. È comunque ammessa l'acquisizione della documentazione di atti che non sono ripetibili. Se la ripetizione dell'atto è divenuta impossibile per fatti o circostanze sopravvenuti, l'acquisizione è ammessa se si tratta di fatti o circostanze imprevedibili. 4. Al di fuori dei casi previsti dai commi 1, 2, 2-bis e 3, i verbali di dichiarazioni possono essere utilizzati nel dibattimento soltanto nei confronti dell'imputato che vi consenta; in mancanza di consenso, detti verbali possono essere utilizzati per le contestazioni previste dagli articoli 500 e 503. 5. Salvo quanto previsto dall'articolo 190-bis, resta fermo il diritto delle parti di ottenere a norma dell'articolo 190 l'esame delle persone le cui dichiarazioni sono state acquisite a norma dei commi 1, 2, 2-bis e 4 del presente articolo». Oltre a poter circolare i documenti come mezzi di prova, possono circolare anche le sentenze irrevocabili sia ai fini dell'accertamento della personalità dell'imputato o della vittima dei reati, sia come prova dei fatti in essi accertati, secondo l'art. 238-bis c.p.p., il quale recita: «1. Fermo quanto previsto dall'articolo 236, le sentenze divenute irrevocabili possono essere acquisite ai fini della prova di fatto in esse accertato e sono valutate a norma degli articoli 187 e 192, comma 3». Ma il fenomeno circolatorio può addirittura riguardare gli atti di indagine: si pensi al collegamento di indagini e al coordinamento tra uffici del Pubblico Ministero che comporta uno scambio frequente di atti regolato dall'art. 371 c.p.p. Tutto ciò attiene alla circolazione probatoria interna e non ha nessuna attinenza con la circolazione probatoria sovranazionale che, invece, attiene alla formazione transfrontaliera della prova.

⁴¹³ Sul tema della fiducia reciproca, si veda, *ex multis*, N. PARISI, *Riconoscimento reciproco delle decisioni giudiziarie penali, confiance mutuelle e armonizzazione delle garanzie procedurali negli Stati membri dell'Unione europea*, in AA.VV., *Scritti in onore di Ugo Draetta*, (a cura di N. PARISI, M. FUMAGALLI MERAVIGLIA, D. RINOLDI, A. SANTINI), Napoli, 2011; S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Giuffrè, 2007; C. AMALFITANO, *sub Art. 82 TFUE*, in AA.VV., *Trattati dell'Unione Europea* (a cura di A. TIZZANO), cit., p. 867 ss.; S. MONTALDO, *On a Collision Course! Mutual Recognition, Mutual Trust and the Protection of Fundamental Rights in the Recent Case-Law of the Court of Justice*, in *European Papers*, 3, 2016, p. 965 ss.; J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 345 ss. Sul rapporto tra reciproca fiducia e richieste di assistenza giudiziaria internazionali, v., G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e *procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012, p. 504 ss.; ID., *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), vol. IV, *Impugnazioni. Esecuzione penale. Rapporti giurisdizionali con autorità straniera* (a cura di L. KALB), Milano, 2015, p. 973 ss. Sulla strumentalità del principio della reciproca fiducia si esprime F. SPIEZIA, *Il coordinamento giudiziario sovranazionale: problemi e prospettive alla luce della nuova decisione 2009/426/GAI che rafforza i poteri di Eurojust*, in *Cass. pen.*, 5, 2010, p. 1991, il quale osserva come il ravvicinamento normativo degli Stati membri sia «strumentale al rafforzamento della mutua fiducia tra le autorità

Invero, tanto il principio della fiducia reciproca tra gli Stati membri quanto il principio del mutuo riconoscimento, che si fonda a sua volta sulla fiducia reciproca tra questi ultimi, rivestono un'importanza fondamentale nel diritto dell'Unione, dato che consentono la creazione e il mantenimento di uno spazio senza frontiere interne⁴¹⁴.

Per “fiducia reciproca” si intende la particolare condotta assunta tra gli Stati membri dell'Unione europea a seguito di una valutazione positiva delle relazioni e della normativa di ogni singolo Stato, che genera un sentimento di sicurezza reciproca, sulla scorta della condivisione dei principi della democrazia e dei diritti umani.

Invero, ogni Stato membro condivide con tutti gli altri Stati, e riconosce che questi condividono con esso, una serie di valori comuni sui quali l'Unione si fonda, così come precisato all'art. 2 TUE. Tale premessa implica e giustifica l'esistenza della fiducia reciproca tra gli Stati membri nel riconoscimento di detti valori e, dunque, nel rispetto del diritto dell'Unione che li attua.

Più specificamente, secondo i più recenti arresti della Corte di giustizia dell'Unione europea, il principio della fiducia reciproca consente a ciascuno Stato membro, segnatamente per quanto riguarda lo spazio di libertà, sicurezza e giustizia, di ritenere, che tutti gli altri Stati membri rispettino il diritto dell'Unione e, più in particolare, i diritti fondamentali riconosciuti da quest'ultimo, eccetto in ipotesi eccezionali⁴¹⁵.

Il riconoscimento di un provvedimento di un'autorità giudiziaria straniera deve fondarsi su un elevato livello di reciproca fiducia tra ordinamenti giuridici che sono o dovrebbero essere in grado di assicurare un elevato *standard* di tutela dei diritti fondamentali tale «da produrre decisioni penali affidabili e, quindi, suscettibili di essere eseguite sul territorio degli altri Paesi senza fare ricorso ad estenuanti ed incerte procedure di riconoscimento»⁴¹⁶. Pertanto, l'Unione europea ha costruito il mutuo riconoscimento fondandolo sulla fiducia reciproca.

La libera circolazione della prova non ne può fare a meno. Appena formulata, era ritenuta presupposto già acquisito dagli Stati membri, in virtù dei principi che condividevano, tant'è che si presumeva che gli ordinamenti giuridici – così com'erano, con i propri principi e con le proprie regole – fossero sufficientemente affidabili per recepire direttamente gli atti provenienti dagli altri Stati membri dell'Unione europea, a differenza dei Paesi esterni all'Unione, nei confronti dei quali vi è ancora oggi una

giudiziarie dei Paesi membri» e rappresenta la «precondizione per una compiuta applicazione degli strumenti basati sul mutuo riconoscimento».

⁴¹⁴ Così, Corte di giustizia, Grande Sezione, sentenza del 17 dicembre 2020, *L. & P.*, cause riunite C-354/20 PPU e C-412/20 PPU, punto 35. In dottrina, D. SIMON, *Mandat d'arrêt européen. Droits fondamentaux dans l'État d'émission*, in *Europe. Actualité du droit de l'Union européenne*, 2, 2021, p. 54 ss.

⁴¹⁵ In tal senso, Corte di giustizia, Grande Sezione, sentenza del 17 dicembre 2020, *L. & P.*, cause riunite C-354/20 PPU e C-412/20 PPU, punto 35; Corte di giustizia, Grande Sezione, sentenza del 15 ottobre 2019, *Dumitru-Tudor Dorobantu*, causa C-128/18, punto 46; Corte di giustizia, Grande Sezione, sentenza del 27 maggio 2019, *OG & PI (Procure di Lubecca e di Zwickau)*, cause C-508/18 e C-82/19 PPU, punto 43; Corte di giustizia, Grande Sezione, sentenza del 25 luglio 2018, *Minister for Justice and Equality/L.M.*, C-216/18, punto 37; Corte di giustizia, Sez. I, sentenza del 25 luglio 2018, *Generalstaatsanwaltschaft Bremen* (Condizioni di detenzione in Ungheria), C-220/18 PPU, punto 49. Cfr., anche, Corte di giustizia, seduta plenaria, parere 2/13, 18 dicembre 2014, punto 191.

⁴¹⁶ Sul punto, v. la Risoluzione del Parlamento europeo sul riconoscimento reciproco delle decisioni definitive in materia penale del 26 luglio 2000, COM (2000) 495 def., *considerando f)*. In dottrina, L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, AA.VV., *L'ordine europeo d'indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 11; A. MANGIARACINA, sub *Art. 696-bis c.p.p.*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), cit., p. 14.

maggior cautela. L'assunto di base è che gli Stati dell'Unione, in fondo, fanno tutti parte del Consiglio d'Europa e quindi condividono i principi contenuti nella Convenzione europea dei diritti dell'uomo⁴¹⁷.

In realtà, prima dell'esplicita formulazione del principio a livello europeo, già i giudici nazionali basavano il mutuo riconoscimento sulla reciproca fiducia. Di *confiance mutuelle* parlava, già nel 1995, la Corte Suprema Spagnola quando, per l'ammissibilità degli elementi di prova raccolti all'estero, applicava il principio del mutuo riconoscimento fondandolo proprio sulla fiducia reciproca⁴¹⁸.

Un anno prima, invece, la Corte di Cassazione italiana sostenne che l'adesione agli atti internazionali comporta «l'implicito riconoscimento della diversità dei singoli ordinamenti e dell'impegno a riconoscere gli atti compiuti secondo i diversi sistemi, in armonia con il principio di prevalenza delle norme pattizie su quelle interne, riconosciuto dall'art. 696 c.p.p.»⁴¹⁹.

Particolarmente interessante è poi l'orientamento tedesco. Nei casi di assistenza giudiziaria la Corte costituzionale tedesca (*Bundesverfassungsgericht*) ha compiuto un importante passo avanti: non applica lo *standard* tedesco comune di tutela dei diritti fondamentali. Piuttosto, rispetta i diversi *standard* di protezione degli altri Paesi e, di conseguenza, è persino disposto a ridurre lo *standard* costituzionale di protezione applicabile al minimo assoluto. La Corte costituzionale giustifica il suo approccio con la fiducia nello "stato di diritto" e la protezione dei diritti umani nello Stato richiedente⁴²⁰.

Dando uno sguardo oltreoceano, si nota un approccio basato su una fiducia (quasi) illimitata nel sistema legale straniero da parte degli Stati Uniti d'America. La "*rule of non-inquiry*"⁴²¹ è stata invocata in un caso riguardante il trasferimento di due cittadini statunitensi dagli USA alla custodia irachena per celebrare il processo nei tribunali di questo Stato. Sebbene i cittadini statunitensi abbiano affermato che probabilmente in Iraq sarebbero stati torturati, la Corte Suprema degli Stati Uniti ha stabilito che «spetta ai rami politici, non alla magistratura, valutare le pratiche nei Paesi stranieri e determinare la politica nazionale alla luce di tali valutazioni»⁴²². In base a questa regola, i tribunali si astengono dall'esaminare se i procedimenti nello Stato richiedente siano equi; inoltre non indagano sulle procedure di trattamento che attendono una persona consegnata nello Stato richiedente⁴²³.

⁴¹⁷ Così J. R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 348.

⁴¹⁸ Corte Suprema Spagnola (penale), decisione del 19 gennaio 1995 – STS 13/1995; Id., decisione del 20 settembre 2005 – STS 1142/2005.

⁴¹⁹ Cass. pen., sez. VI, sentenza del 4 marzo 1994, Palamara, in *Cass. pen.*, 1995, p. 2647. Nello stesso senso, più di recente, un'altra sentenza delle sezioni unite, Cass. pen., Sez. Un., sentenza del 25 febbraio 2010, Mills, par. 10.4, in *Cass. pen.*, 2010, p. 3008.

⁴²⁰ Nel caso specifico si trattava di un rapporto con l'autorità Russa. Cfr., BVerfG, 20 dicembre 2007, 2 BvR 1996/07, Rn. 19. V. anche H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, cit., p.47.

⁴²¹ Per un'analisi relativa al contesto storico e all'applicazione del "*Rule of non-inquiry*", J.T. PARRY, *International Extradition, the Rule of Non-Inquiry and the Problem of Sovereignty*, in *Boston University Law Review*, 2010, p. 1973 ss.

⁴²² Cfr., US Supreme Court's decision in *Munaf v. Geren*, 553 U.S. 674 (2008).

⁴²³ Sul punto, M. MURCHISON, *Extradition's Paradox: Duty, Discretion, and Rights in the World of Non-Inquiry*, in *Stanford Journal of International Law*, 2, 2007, p. 295 ss., con ulteriori indicazioni della giurisprudenza sull'argomento; H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, cit., p. 48.

Orbene, la fiducia reciproca può comportare due conseguenze diverse: o vuol dire che gli Stati devono recepire automaticamente tutti gli atti provenienti da un altro Stato perché la fiducia è implicita; o vuol dire che il mutuo riconoscimento deve fondarsi su una reciproca fiducia, in quanto nei sistemi penali degli Stati vi è una comunanza di “*standard qualitativi*”⁴²⁴ tali da poterla giustificare.

Infatti, la dottrina ha osservato che «le garanzie procedurali individuali assicurate entro gli ordinamenti nazionali ai fini della celebrazione del processo penale rappresentano il banco di prove del funzionamento del reciproco riconoscimento»⁴²⁵. Se così è, però, è necessario individuare una normativa minima comune tra gli Stati membri che in origine sicuramente mancava. A causa di tale assenza, si potrebbe generare una crisi della fiducia reciproca e del mutuo riconoscimento qualora gli Stati non corrano ai ripari uniformando o armonizzando le norme che riguardino le garanzie per gli imputati e per le vittime nel processo penale⁴²⁶.

Il problema, in fondo, è che sancire astrattamente la reciproca fiducia negli atti dell'Unione europea⁴²⁷ non esclude il rischio che il mutuo riconoscimento fallisca, poiché è necessario che la fiducia, per essere “effettiva”, si concretizzi in un serio ravvicinamento delle normative nazionali⁴²⁸. Difatti la fiducia più che data per scontata, va conquistata,

⁴²⁴ La terminologia è mutuata da J. R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 348.

⁴²⁵ In questi termini N. PARISI, *Riconoscimento reciproco delle decisioni giudiziarie penali, confiance mutuelle e armonizzazione delle garanzie procedurali negli Stati membri dell'Unione europea*, in AA.VV., *Scritti in onore di Ugo Draetta* (a cura di N. PARISI, M. FUMAGALLI MERAVIGLIA, D. RINOLDI, A. SANTINI), cit., p. 505.

⁴²⁶ Il riferimento è alla direttiva 2012/29/EU, che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato, e che sostituisce la decisione quadro 2001/220/GAI. Al riguardo, si veda E. CANNIZZARO, *La riparazione dei danni da attività giudiziaria nel diritto dell'Unione europea*, in AA.VV., *La vittima del processo. I danni da attività processuale penale* (a cura di G. SPANGHER), Torino, 2017, p. 73 ss.; A. IERMANO, *La tutela delle vittime di reato nello “spazio procedurale-processuale penale”: la direttiva 2012/29/UE*, in *Rivista della cooperazione giuridica internazionale*, 45, 2013, p. 125 ss.; M. SIMONATO, *Deposizione della vittima e giustizia penale. Una lettura del sistema italiano*, Padova, 2014, p. 103 ss. Sulla direttiva, v. anche, volendo, A. GAUDIERI, *Corte cost., 21 febbraio – 27 aprile 2018, n. 92*, in AA.VV., *Corte costituzionale e sistema processuale penale. L'elaborazione giurisprudenziale del 2018* (a cura di D. CIMADOMO, G. DALIA), cit., p. 143 ss.

⁴²⁷ Il riferimento è in particolare al Preambolo del Programma dell'Unione europea concernente misure per l'attuazione del principio del reciproco riconoscimento delle decisioni penali adottato dal Consiglio il 12 novembre 2000 in GUCE n. C 012/02 del 15 gennaio 2001 e alla decisione quadro 2002/584/GAI del 13 giugno 2002 che ha istituito il mandato di arresto europeo in GUUE L-190/1 del 18 luglio 2002.

⁴²⁸ G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. *Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), cit., p. 537; ID., *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), cit., p. 1073; D. CURTOTTI, *Le procedure di consegna della persona: b) il mandato di arresto europeo*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), IV, *Le impugnazioni. Esecuzione penale. Rapporti giurisdizionali con autorità straniere* (a cura di L. KALB), Torino, 2015, p. 973 ss.; in tema, anche F. SPIEZIA, *Il coordinamento giudiziario sovranazionale: problemi e prospettive alla luce della nuova decisione 2009/426/GAI che rafforza i poteri di Eurojust*, in *Cass. pen.*, 5, 2010, p. 1991, il quale osserva come il ravvicinamento normativo degli Stati membri sia «strumentale al rafforzamento della mutua fiducia tra le autorità giudiziarie dei Paesi membri» e rappresenta la «precondizione per una compiuta applicazione degli strumenti basati sul mutuo riconoscimento». Il nesso di strumentalità tra ravvicinamento delle disposizioni legislative nazionali e il mutuo riconoscimento delle decisioni è efficacemente descritto anche da G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in *Cass. pen.*, 1, 2006, p. 272 con la seguente osservazione: «L'attuazione del principio del mutuo riconoscimento delle decisioni giudiziarie non può svilupparsi soltanto sul binario della definizione delle norme procedurali necessarie ad assicurare l'esecuzione nel territorio di uno Stato membro delle decisioni

ed una volta conquistata, rappresenta la «chiave del buon funzionamento dei meccanismi semplificati»⁴²⁹: diventa, cioè, l'elemento determinante per semplificare tutti i procedimenti e gli strumenti della cooperazione giudiziaria.

Ma ciò non può avvenire se alla base non si eliminano tutte le sovrastrutture che innestano fattori di diffidenza tra Stati. L'unico modo per ovviare a ciò sarebbe la creazione di una normativa minima comune, una armonizzazione delle norme minime.

Invero, se le differenze relative alle leggi applicabili sono considerevoli e/o se i sistemi giuridici hanno caratteristiche incomparabili, se la storia, la lingua e la tradizione giuridica differiscono, il riconoscimento reciproco necessita di fattori "complementari" aggiuntivi al fine di creare una base oggettiva per la fiducia reciproca. Tali fattori possono essere generati dall'armonizzazione della legislazione. Inoltre, deve essere garantito il rispetto di una base comune di diritti fondamentali nelle procedure penali nonché la *rule of law* e la prevedibilità degli orientamenti giurisprudenziali⁴³⁰.

In realtà, tra gli Stati membri sembra esservi un vero e proprio *deficit* di fiducia reciproca specialmente riguardo a politiche di cooperazione giudiziaria e di polizia in questioni penali⁴³¹. Vi è ormai piena consapevolezza che la reciproca fiducia deve essere sempre più reale. Presupporla è stato un errore manifestatosi con tutta evidenza proprio con l'approvazione della decisione quadro relativa al mandato di arresto europeo, la quale ha generato in molti, se non in tutti i Paesi, forti discussioni, malumori, perplessità e obiezioni a causa delle preoccupazioni destinate dal livello non particolarmente soddisfacente della giustizia penale di alcuni Stati membri, tant'è che la decisione quadro ha atteso tempi biblici prima che venisse recepita in tutti gli Stati.

Si è capito che la fiducia reciproca, ritenuta sinora un "dogma assoluto", così scontata non era. Era necessario rifondare la reciproca fiducia partendo dall'individuazione di norme minime comuni a tutti gli Stati membri, sul presupposto che essa non è elemento statico, ma criterio dinamico⁴³².

Il difficile equilibrio da individuare tra reciproca fiducia e rispetto dei diritti fondamentali è stato oggetto di una intensa attività ermeneutica della Corte di giustizia dell'Unione europea. In principio, la Corte assolutizzò la fiducia reciproca, e pertanto

giudiziarie assunte da autorità di un altro Stato membro. Una pur limitata prospettiva di integrazione normativa è essenziale al funzionamento di un sistema di cooperazione fondato sul principio del mutuo riconoscimento, poiché soltanto l'espansione del nucleo di regole di diritto sostanziale e processuale condivise consente di praticare effettivamente la fiducia verso gli altri sistemi giuridici che è alla base del principio del mutuo riconoscimento delle decisioni giudiziarie».

⁴²⁹ Così S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007, p. 694.

⁴³⁰ Diversamente, se rimangono solo piccole differenze, soprattutto se gli Stati interessati fanno parte della stessa "famiglia legale", se condividono la stessa tradizione giuridica, mentalità giuridica e valori, se entrambi accettano una serie comparabile di diritti fondamentali, se hanno un comune storia e forse anche un linguaggio simile, la base oggettiva della fiducia reciproca può essere applicata, anche senza limitazioni e disposizioni di ordine pubblico. Sul punto, H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, cit., p. 55.

⁴³¹ Cfr. la Risoluzione del Parlamento europeo del 25 settembre 2008, relativa al "dibattito annuale sui progressi compiuti nello spazio di libertà, sicurezza e giustizia (art. 2 e 39 del Trattato UE)", sul sito internet www.europarl.europa.eu.

⁴³² Questo imporrebbe di controllare e "vegliare" costantemente sulla situazione giuridica degli altri paesi. In caso di eventi imprevisti e deprecabili come, ad esempio, un continuo mancato rispetto dei diritti fondamentali o una crisi costituzionale, cambierebbero le basi della fiducia reciproca (ecco il dinamismo), per cui lo Stato dovrebbe intervenire o porre fine alla cooperazione.

privilegiò l'efficienza della cooperazione giudiziaria rispetto ai diritti fondamentali della persona raggiunta da un mandato di arresto europeo⁴³³.

In particolare, a parere della Corte, la cooperazione giudiziaria ha lo scopo di contribuire a realizzare l'obiettivo assegnato all'Unione di diventare uno spazio di libertà, sicurezza e giustizia fondandosi sull'elevato livello di fiducia che deve esistere tra gli Stati membri⁴³⁴. In tal senso, non sembrerebbe sussistere alcun margine di valutazione da parte di uno Stato relativamente al rischio di lesione dei diritti fondamentali. L'autorità di esecuzione, in virtù di un presunto elevato livello di fiducia, non potrebbe dubitare dell'altrui osservanza dei diritti delle persone sottoposte a procedimento penale⁴³⁵.

Con la sentenza *Melloni*, la Corte continuava a difendere un concetto radicale di reciproca fiducia. Infatti, nello stabilire che lo Stato di esecuzione può subordinare la consegna della persona raggiunta da un MAE unicamente al rispetto degli *standard* minimi individuati dal diritto dell'Unione europea e non anche – o solamente – all'osservanza del più alto livello di tutela dei diritti così come stabilito dal proprio ordinamento nazionale, ha osservato che «permettere ad uno Stato membro di valersi dell'articolo 53 della Carta per subordinare la consegna di una persona condannata *in absentia* alla condizione, non prevista dalla decisione quadro 2009/299, che la sentenza di condanna possa essere oggetto di revisione nello Stato membro emittente, al fine di evitare una lesione del diritto ad un processo equo e dei diritti della difesa garantiti dalla Costituzione dello Stato membro di esecuzione, comporterebbe, rimettendo in discussione l'uniformità dello *standard* di tutela dei diritti fondamentali definito da tale decisione quadro, una lesione dei principi di fiducia e riconoscimento reciproci che essa mira a rafforzare e, pertanto, un pregiudizio per l'effettività della suddetta decisione quadro»⁴³⁶.

⁴³³ Cfr., Corte di giustizia, Grande sezione, sentenza del 29 gennaio 2013, *Ciprian Vasile Radu*, causa C-396/11. In dottrina, A. MANGIARACINA, sub *Art. 696-ter c.p.p.*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 26. Per un commento alla sentenza *Radu*, V. ALTAMORE, "Mandato di arresto europeo" e "diritti fondamentali": dall'assolutezza alla negoziabilità dei diritti fondamentali? *Spunti di riflessione in una recente sentenza della Corte di giustizia*, in *Diritto pubblico comparato ed europeo*, 2013, p. 602 ss.; C. BRIÈRE, *La jurisprudence de la Cour de justice et du Tribunal de l'Union européenne. Chronique des arrêts. Arrêt «Radu»*, in *Revue du droit de l'Union européenne*, 1, 2013, p. 171 ss.; R. STEFANOVA-KAMISHEVA, *Zashtita na osnovnite prava na choveka pri izpalnenie na evropeyskata zapoved za arest*, in *Evropeyski praven pregled*, 6, 2013, p. 163 ss.; A. TINSLEY, *The Reference in Case C-396/11 Radu: When does the Protection of Fundamental Rights Require Non-execution of a European Arrest Warrant?*, in *European Criminal Law Review*, 2012, p. 338 ss.

⁴³⁴ In tal senso, Corte di giustizia, Sez. II, sentenza 28 giugno 2012, *West*, causa C-192/12 PPU, punto 53.

⁴³⁵ Così, S. CIVELLO CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell'Unione Europea*, cit., p. 9.

⁴³⁶ Cfr. Corte di giustizia, Grande sezione, sentenza del 26 febbraio 2013, *Stefano Melloni c. Ministero Fiscal*, C-399/11, par. 63. Per un commento alla sentenza *de qua*, D. ACHILLE, *Primato del diritto europeo e tutela dei diritti fondamentali nel sistema ordinamentale integrato*, in *Nuova giur. civ.*, 12, 2018, p. 1890 ss.; C. AMALFITANO, *Mandato d'arresto europeo: reciproco riconoscimento vs diritti fondamentali? Note a margine delle sentenze Radu e Melloni della Corte di giustizia*, in *penalecontemporaneo.it*, 4 luglio 2013, disponibile al link: <https://archivioldpc.dirittopenaleuomo.org/d/2402-mandato-d-arresto-europeo--reciprocoriconoscimento-vs-diritti-fondamentali>; S. CIVELLO CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell'Unione europea. Un commento alle sentenze Radu e Melloni della Corte di giustizia*, in *penalecontemporaneo.it*, cit.; G. DE AMICIS, *All'incrocio tra diritti fondamentali, mandato d'arresto europeo e decisioni contumaciali: la Corte di Giustizia e il "caso Melloni"*, in *penalecontemporaneo.it*, 7 giugno 2013; N. DE BOER, *Addressing rights divergences under the Charter: Melloni*, in *Common Market Law Review*, 4, 2013, p. 1083 ss.; T. EPIDENDIO, *Il caso Melloni: il nodo irrisolto del massimo standard di tutela dei diritti fondamentali*, in

Il fondamento risiede nel principio del primato del diritto dell'Unione europea, che verrebbe inficiato qualora la consegna di una persona raggiunta da un mandato di arresto europeo fosse subordinata al vaglio di un giudice sul rispetto dei diritti fondamentali previsti dalle norme interne e dalla Costituzione nazionale, sminuendo così l'efficacia del diritto dell'Unione⁴³⁷.

Con il parere 2/2013, la Corte di Lussemburgo, nel continuare la sua difesa nei confronti di una rigida interpretazione della fiducia reciproca, opera una timida apertura verso una maggior considerazione dei diritti fondamentali. Secondo la Corte, il principio

Quaderni costituzionali, 2, 2013, p. 451 ss.; V. FAGGIANI, *La sentenza del TC sul caso Melloni: esempio del dialogo giudiziario europeo o di un monologo?*, in *forumcostituzionale.it*, 20 marzo 2015, disponibile al link: <http://www.forumcostituzionale.it/wordpress/wp-content/uploads/2015/03/faggiani.pdf>; T. FENUCCI, *A proposito della Corte di giustizia UE e dei c.d. "controlimiti": i casi Melloni e Taricco a confronto*, in *Freedom, Security & Justice Review*, 1, 2018, p. 95 ss.; G. LATTANZI, *Il dialogo tra le Corti nei casi Melloni e Taricco*, in *Cass. pen.*, 6, 2017, p. 2131B ss.; S. MANACORDA, *Dalle carte dei diritti a un diritto penale "à la carte"*, in *penalecontemporaneo.it*, 17 maggio 2013, disponibile al link: <https://archivioldpc.dirittopenaleuomo.org/d/2290-dalle-carte-dei-diritti-a-un-diritto-penale-a-la-carte>; A. RUGGERI, *La Corte di giustizia e il bilanciamento mancato (a margine della sentenza Melloni)*, in *Il Diritto dell'Unione europea*, 2, 2013, p. 399 ss.; V. SKOURIS, *Développements récents de la protection des droits fondamentaux dans l'Union européenne: les arrêts Melloni et Åkerberg Fransson*, in *Il Diritto dell'Unione europea*, 2, 2013, p. 229 ss.; F. VIGANÒ, *Obblighi di adeguamento al diritto UE e "controlimiti": la Corte costituzionale spagnola si adegua, bon gré mal gré, alla sentenza dei giudici di Lussemburgo nel caso Melloni*, in *penalecontemporaneo.it*, 9 marzo 2014, disponibile al link: <https://archivioldpc.dirittopenaleuomo.org/d/2865-obblighi-di-adeguamento-al-diritto-ue-e-controlimiti--la-corte-costituzionale-spagnola-si-adequa-b>; U. VILLANI, *Istituzioni di diritto dell'Unione europea*, Bari, 2020, p. 62 ss. Inoltre, sul punto v. anche, A. DA FONSECA, *Le Tribunal constitutionnel espagnol et la Cour de justice: un dialogue d'apparat autour de l'affaire Melloni?*, in *gdr-elsj.eu*, 30 marzo 2014, disponibile al link: <http://www.gdr-elsj.eu/2014/03/30/cooperation-judiciaire-penale/le-tribunalconstitutionnel-espagnol-et-la-cour-de-justice-un-dialogue-dapparat-autour-de-laffaire-melloni/>; H. LABAYLE, *Mandat d'arrêt européen et degré de protection des droits fondamentaux, quand la confiance se fait aveugle*, in *gdr-elsj.eu*, 3 marzo 2013, disponibile al link: <http://www.gdr-elsj.eu/2013/03/03/cooperation-judiciaire-penale/mandat-darret-europeen-et-degre-de-protection-des-droits-fondamentaux-quand-la-confiance-se-fait-aveugle/>; R. MEDHI, *Retour sur l'arrêt Melloni: quelques réflexions sur des usages contradictoires du principe de primauté*, in *gdr-elsj.eu*, 29 marzo 2013, disponibile al link: <http://www.gdr-elsj.eu/2013/03/29/cooperation-judiciaire-penale/retour-surlarret-melloni-quelques-reflexions-sur-des-usages-contradictaires-du-principe-de-primaute/>; N.M. SCHALLMOSER, *The European Arrest Warrant and Fundamental Rights. Risks of Violations of Fundamental Rights through the EU Framework Decision in Light of the ECHR*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2, 2014, p. 146.

⁴³⁷ Cfr. Corte di giustizia, Grande sezione, *Melloni*, cit., par. 59; Corte di giustizia, Grande sezione, sentenza del 8 settembre 2010, *Winner Wetten GmbH c. Bürgermeisterin der Stadt Bergheim*, C-409/06, par. 61. Inoltre, è noto come l'art. 51, par. 2, Carta dei diritti fondamentali dell'Unione europea si applichi a tutte le norme europee nonché alle norme nazionali che ricadano nell'ambito di applicazione del diritto europeo. Cfr., Corte di giustizia, Grande Sezione, sentenza del 26 febbraio 2013, *Åkerberg Fransson*, C-617/10, par. 21-22: «dato che i diritti fondamentali garantiti dalla Carta devono essere rispettati quando una normativa nazionale rientra nell'ambito di applicazione del diritto dell'Unione, non possono [...] esistere casi rientranti nel diritto dell'Unione senza che tali diritti fondamentali trovino applicazione. L'applicabilità del diritto dell'Unione implica quella dei diritti fondamentali garantiti dalla Carta. Ove, per contro, una situazione giuridica non rientri nella sfera d'applicazione del diritto dell'Unione, la Corte non è competente al riguardo e le disposizioni della Carta eventualmente richiamate non possono giustificare, di per sé, tale competenza». In dottrina, E. CANNIZZARO, *La cornice europea*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018 (a cura di L. KALB), Milano, 2019, p. 38. Per un approfondimento della giurisprudenza recente sul tema, A. RASI, *Effetti indiretti della Carta dei diritti fondamentali? In margine alla sentenza Commissione c. Polonia (Indépendance de la Cour suprême)*, in *European Papers – European Forum*, 31 luglio 2019, recuperabile al link: <https://www.europeanpapers.eu/en/europeanforum/effetti-indiretti-della-carta-dei-diritti-fondamentali-sentenza-commissione-polonia>.

della reciproca fiducia riveste nel diritto dell'Unione europea un'importanza fondamentale per la creazione di uno spazio di libertà, sicurezza e giustizia senza frontiere interne, ed impone a ciascuno Stato di ritenere, tranne in circostanze eccezionali, che tutti gli altri Stati membri rispettano il diritto dell'Unione ed in particolare i diritti fondamentali da questa riconosciuti.

«Allorché attuano il diritto dell'Unione, gli Stati membri possono quindi essere tenuti, in forza di quest'ultimo, a presumere il rispetto dei diritti fondamentali da parte degli altri Stati membri, sicché risulta ad essi preclusa non soltanto la possibilità di esigere da un altro Stato membro un livello di tutela nazionale dei diritti fondamentali più elevato di quello garantito dal diritto dell'Unione, ma anche, salvo casi eccezionali, quella di verificare se tale altro Stato membro abbia effettivamente rispettato, in un caso concreto, i diritti fondamentali garantiti dall'Unione»⁴³⁸. Proprio il riferimento alle circostanze eccezionali rappresenta la chiave di volta per interpretazioni innovative.

Ed invero, più di recente si è detto che il principio della reciproca fiducia imponga agli Stati membri di presumere che gli altri Stati rispettino il diritto dell'Unione europea e, nello specifico, i diritti fondamentali riconosciuti da esso (salvo circostanze eccezionali). Dunque, la garanzia della tutela dei diritti della persona di cui è stata chiesta la consegna rientra nella responsabilità dello Stato membro emittente. Pertanto, si deve presumere che il medesimo osservi il diritto dell'Unione ed i diritti fondamentali riconosciuti da quest'ultimo⁴³⁹. Si ritiene, quindi, che tale presunzione di conformità sia relativa⁴⁴⁰.

Una discontinuità rispetto agli orientamenti passati si nota anche nella sentenza *Aranyosi e Căldăraru*⁴⁴¹, con la quale si assiste ad un'apertura verso la tutela dei diritti fondamentali quali limite alla reciproca fiducia, dilatando la tutela dei diritti fondamentali.

La Corte di giustizia, dopo aver riaffermato la fondamentale importanza rivestita dal principio della reciproca fiducia e del mutuo riconoscimento nel diritto dell'Unione europea, in quanto consentono la creazione e il mantenimento di uno spazio senza frontiere interne, conferma che l'autorità giudiziaria di esecuzione può rifiutarsi soltanto nei casi tassativamente elencati di non esecuzione obbligatoria o di non esecuzione facoltativa⁴⁴². Però, virando rispetto ai precedenti orientamenti, ammette che possono essere apportate limitazioni ai principi del mutuo riconoscimento e di fiducia reciproca tra Stati membri “in circostanze eccezionali” quando lo esige il rispetto dei diritti fondamentali, eliminando così qualsiasi automatismo nell'applicazione.

⁴³⁸ Cfr., Corte di giustizia, seduta plenaria, parere 2/13, 18 dicembre 2014, punto 192.

⁴³⁹ Il tema è stato già ampiamente affrontato in, Corte di giustizia, Grande sezione, sentenza del 23 gennaio 2018, *Piotrowski*, C-367/16, par. 50. Ivi, i giudici hanno ritenuto che «Tuttavia, nel caso di un procedimento riguardante un mandato d'arresto europeo, la garanzia di tali diritti spetta in primo luogo allo Stato membro emittente, che si deve presumere rispetti il diritto dell'Unione e, in particolare, i diritti fondamentali riconosciuti da quest'ultimo».

⁴⁴⁰ Cfr., *considerando* 19, direttiva 2014/41/UE.

⁴⁴¹ Corte di giustizia, Grande sezione, sentenza del 5 aprile 2016, *Aranyosi e Căldăraru*, C-404/15 e C-659/15.

⁴⁴² Cfr., Corte di giustizia, Grande Sezione, sentenza del 16 luglio 2015, *Minister for Justice and Equality contro Francis Lanigan*, C-237/15 PPU, par. 36; Corte di giustizia, Sez. II, sentenza del 28 giugno 2012, *Melvin West*, C-192/12 PPU, par. 55; Corte di giustizia, Grande sezione, *Melloni*, cit., par. 38; Corte di giustizia, Sez. II, sentenza del 30 maggio 2013, *Jeremy F. contro Premier ministre*, C-168/13 PPU, par. 36.

Si tratta, quindi, di un primo passo della Corte verso una attenzione maggiore, se non piena, ai diritti fondamentali, i quali vanno pian piano posizionandosi al centro dell'argomentazione dei giudici di Lussemburgo.

Dopo aver riconosciuto al divieto di trattamenti inumani o degradanti un carattere assoluto, lapidariamente affermano che: «quando l'autorità giudiziaria dello Stato membro d'esecuzione dispone di elementi che attestano un rischio concreto di trattamento inumano o degradante dei detenuti nello Stato membro emittente, tenuto conto del livello di tutela dei diritti fondamentali garantito dal diritto dell'Unione e, in particolare, dall'articolo 4 della Carta, essa è tenuta a valutare la sussistenza di tale rischio quando decide in ordine alla consegna alle autorità dello Stato membro emittente della persona colpita da un mandato d'arresto europeo»⁴⁴³. Spetterà, allora, al giudice nazionale valutare la sussistenza di tale rischio e, in ragione di ciò, decidere di conseguenza⁴⁴⁴.

Ulteriore tassello è stato aggiunto dalla sentenza *Dorobantu*⁴⁴⁵, con la quale la Corte di Lussemburgo ha imposto una nuova centralità ai diritti fondamentali, basati sul concetto di dignità umana. Proprio il carattere assoluto del divieto di trattamenti inumani e degradanti prescrive, al fine di decidere sulla consegna di una persona raggiunta da un mandato di arresto europeo, di non procedere ad alcun bilanciamento con il principio di reciproca fiducia, con il principio del mutuo riconoscimento e con considerazioni relative

⁴⁴³ Tale accertamento deve «fondarsi su elementi oggettivi, attendibili, precisi e opportunamente aggiornati sulle condizioni di detenzione vigenti nello Stato membro emittente e comprovanti la presenza di carenze vuoi sistemiche o generalizzate, vuoi che colpiscano determinati gruppi di persone, vuoi ancora che colpiscano determinati centri di detenzione. Tali elementi possono risultare in particolare da decisioni giudiziarie internazionali, quali le sentenze della Corte EDU, da decisioni giudiziarie dello Stato membro emittente, nonché da decisioni, relazioni e altri documenti predisposti dagli organi del Consiglio d'Europa o appartenenti al sistema delle Nazioni Unite».

⁴⁴⁴ Il giudice è, dunque, tenuto a eseguire un «two-step test» in base al quale dovrà prima determinare se sussistano elementi oggettivi, attendibili, precisi e debitamente aggiornati tendenti a testimoniare l'esistenza di un rischio reale di violazione dei diritti fondamentali a causa di carenze sistemiche o generalizzate ed, in una seconda fase, procedere a verificare, in modo concreto e preciso, in quale misura tali carenze siano idonee ad avere un impatto a livello degli organi giurisdizionali dello Stato membro competenti a conoscere del procedimento e se, alla luce della situazione individuale della persona, della natura del reato per il quale di procede e del contesto fattuale in cui si inserisce l'attività, e tenuto conto delle informazioni eventualmente fornite dallo Stato membro richiedente, esistono motivi seri e comprovati di ritenere che la persona corra un rischio. Cfr., Corte di giustizia, Prima sezione, sentenza del 25 luglio 2018, *Minister for Justice and Equality (Carenze del sistema giudiziario)*, causa C-216/18 PPU, punti 61, 74 e 77. Le due fasi di tale esame implicano un'analisi dell'informazione ottenuta sulla base di criteri differenti, ragion per cui tali fasi non possono confondersi. Così, Corte di giustizia, Grande Sezione, sentenza del 17 dicembre 2020, *L. & P.*, cause riunite C-354/20 PPU e C-412/20 PPU, punto 56. In dottrina, S. GÁSPÁR-SZILÁGYI, *Joined Cases Aranyosi and Caldáru: Converging Human Rights Standards, Mutual Trust and a New Ground for Postponing a European Arrest Warrant*, in *European journal of Crime, criminal Law and criminal Justice*, 24, 2016, p. 197 ss.; L. PANELLA, *Mandato di arresto europeo e protezione dei diritti umani: problemi irrisolti e "incoraggianti" sviluppi giurisprudenziali*, in *Freedom, Security and Justice: European Legal Studies*, 3, 2017, p. 5 ss.

⁴⁴⁵ Corte di giustizia, Grande Sezione, sentenze del 15 ottobre 2019, *Dumitru-Tudor Dorobantu*, causa C128/18. Per un commento, A. CAIOLA, *Retour sur la mise en œuvre du mandat d'arrêt européen: le respect de l'interdiction des traitements inhumains ou dégradants dans la détention*. CJUE, gde ch., 15 octobre 2019, *Dumitru-Tudor Dorobantu/Hanseatisches Oberlandesgericht Hamburg*, C-128/18, ECLI:EU:C:2019:857, in *Revue des affaires européennes*, 4, 2019, p. 785 ss.; C. RIZCALLAH, *Arrêt «Dorobantu»: mandat d'arrêt européen et exigences minimales relatives aux conditions de détention*, in *Journal de droit européen*, 2, 2020, p. 62 ss. Sia inoltre consentito il rinvio ad A. GAUDIERI, *Sovraffollamento carcerario: i criteri dettati dalla sentenza Dorobantu per il calcolo degli spazi. Una "bussola" per le scelte da compiere in periodo di emergenza sanitaria?*, in *Freedom, Security & Justice Review*, 2, 2020, p. 213 ss.

all'efficacia della cooperazione giudiziaria in materia penale, qualora un giudice constati l'esistenza di seri e comprovati motivi di ritenere che la persona oggetto del mandato di arresto europeo correrà un rischio reale di essere sottoposta a un trattamento inumano o degradante, chiudendo di fatto all'applicazione del principio di proporzionalità⁴⁴⁶.

Questa visione "dignitocentrica" ha consentito alla Corte di giustizia finanche di escludere una valutazione basata sulla tecnica del bilanciamento qualora dovesse essere riscontrato per la persona raggiunta dal mandato d'arresto un rischio reale di un trattamento inumano o degradante, in quanto diritto fondamentale assoluto, e dunque, non limitabile in alcun modo ed in nessun caso⁴⁴⁷.

Ulteriore obiettivo è, quindi, quello di avvicinare i sistemi penali e giudiziari degli Stati membri dell'Unione europea, pur nel rispetto delle proprie diversità e specificità, individuando, attraverso una "tabella di marcia", i principi comuni a tutti i sistemi processuali dei singoli Stati⁴⁴⁸. Tali misure hanno sicuramente una funzione servente al mutuo riconoscimento, consentendogli di essere effettivo.

La fiducia reciproca oltre ad essere un elemento necessario per il mutuo riconoscimento diventa un vero e proprio obiettivo da perseguire. Gli organi dell'Unione europea sono consapevoli dell'instabilità di tale presupposto che faccia da pilastro all'intera struttura del mutuo riconoscimento. Essa è collante imprescindibile per un pieno ed effettivo sviluppo di una giustizia comune nello spazio giudiziario europeo⁴⁴⁹.

Si deve concludere, allora, che la fiducia reciproca resta un elemento fondamentale ed indispensabile per sviluppare in modo soddisfacente il mutuo riconoscimento. Elemento fondamentale, "minimo comune denominatore" necessario, ma non sufficiente, soprattutto in ambito probatorio. A ben vedere, infatti, risulta opportuno che vi sia una preventiva armonizzazione delle regole probatorie minime, necessarie per l'utilizzazione degli elementi di prova stessi⁴⁵⁰, un'interazione tra armonizzazione e fiducia reciproca che non sfoci mai in contrasto o sovrapposizione dell'una sull'altra.

⁴⁴⁶ Cfr., Grande Sezione, sentenze del 15 ottobre 2019, *Dumitru-Tudor Dorobantu*, causa C128/18, punto 84.

⁴⁴⁷ Si tratta, dunque, di un'evoluzione della giurisprudenza, costantemente attenta al sentire sociale dei cittadini dell'Unione europea. Essa ha dimostrato una profonda e sempre crescente sensibilità nei confronti dei diritti umani, orientando assiologicamente le proprie decisioni, anche alla luce degli arresti giurisprudenziali della Corte europea dei diritti dell'uomo. Si assiste ad una prevalenza dei diritti della persona rispetto ad automatismi rivelatisi nel tempo teleologicamente inadeguati, poiché basati su valutazioni in astratto, totalmente scollate dall'ontologico contesto in cui dovrebbero essere calate. Una valutazione in concreto, assiologicamente orientata da canoni, principi e diritti stabiliti anche dalla Carta dei diritti fondamentali dell'uomo, consente di arrivare a soluzioni che, seppur lascerebbero in capo ai giudici un discreto margine di discrezionalità, rendono la decisione simile ad un abito cucito su misura, perfettamente calzante al caso in esame.

⁴⁴⁸ In tal senso O. MAZZA, *Il garantismo al tempo del giusto processo*, cit., p. 55 ss.; S. SIRACUSANO, *Tra mutuo riconoscimento e armonizzazione preventiva: quali prospettive per la circolazione della prova dichiarativa nell'ambito dell'U.E.?*, cit., p. 1 ss.; G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. *Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), cit., p. 525 ss.

⁴⁴⁹ Cfr. A. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 694.

⁴⁵⁰ Di tale avviso è R. DEL COCO, *Ordine europeo di indagine e poteri sanzionatori del giudice*, in *penalecontemporaneo.it*, 21 dicembre 2015. Sui rapporti tra mutuo riconoscimento e armonizzazione, si veda, *ex multis*, S. ALLEGREZZA, *L'armonizzazione della prova penale alla luce del Trattato di Lisbona*, in *Cass. pen.*, 10, 2008, p. 3882 ss.; M. BARGIS, *La cooperazione giudiziaria penale nell'Unione europea tra mutuo riconoscimento e armonizzazione: analisi e prospettive*, cit., p. 914; S. GLESS, *Strategie e tecniche per l'armonizzazione della prova*, in AA.VV., *Prova penale e Unione europea* (a cura di G. ILLUMINATI),

Tale attività rappresenterebbe il collante tra fiducia reciproca e mutuo riconoscimento, saldatura tra due concetti che attendono di fondersi, al fine di raggiungere gli scopi prefissati dallo spazio di libertà, sicurezza e giustizia, punto di equilibrio tra due valori funzionalmente previsti per una cooperazione giudiziaria sempre più efficiente.

9. Il principio del mutuo riconoscimento tra uniformazione e armonizzazione

La dottrina ritiene che per combattere la criminalità organizzata transnazionale siano possibili due tipi di approcci: l'approccio orizzontale e l'approccio verticale⁴⁵¹.

La soluzione (o approccio) orizzontale prevede un limitato intervento dell'Unione europea consistente in una semplice attività di coordinamento, lasciando agli Stati membri, i quali applicano le proprie leggi, il compito di intervenire con la cattura e il processo degli autori di reato. Tipico esempio di tale approccio è il principio del mutuo riconoscimento.

A questo si contrappone l'approccio verticale, suddiviso in approccio verticale in senso forte e approccio verticale in senso debole. Quando si parla di approccio verticale in senso forte ci si riferisce all'uniformazione normativa, mentre quando si parla di approccio verticale in senso debole il riferimento è all'armonizzazione o ravvicinamento delle legislazioni nazionali.

Per uniformazione normativa si intende l'insieme di norme di fonte Europea direttamente applicabili all'interno dei singoli Stati membri che possono essere eventualmente attuate da una autorità centrale. Un esempio di uniformazione normativa è L'EPPO⁴⁵², ovvero l'Olaf, l'Ufficio antifrode dell'Unione europea, una agenzia

Bologna, 2009, p. 141 ss.; B. HECKER, *Mutual Recognition and Transfer of Evidence. The European Evidence Warrant*, in AA.VV., *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (coordinato da S. RUGGERI), Heidelberg, 2013, p. 269 ss.; L. MARAFIOTI, *Armonización y proceso penal europeo: la perspectiva italiana*, in AA.VV., *Miscellanea sul fenomeno giuridico* (a cura di V. MANNINO), Napoli, 2012, p. 23 ss.; M.R. MARCHETTI, *Dalla Convenzione di assistenza giudiziaria in materia penale dell'Unione europea al mandato europeo di ricerca delle prove e all'ordine di indagine penale*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), Milano, 2011, p. 135 ss.; F. SIRACUSANO, *Tra mutuo riconoscimento e armonizzazione preventiva: quali prospettive per la prova dichiarativa nell'ambito dell'Unione europea?*, cit., p. 1 ss.; G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., *«Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), cit., p. 524 ss.

⁴⁵¹ J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea*, (a cura di R.E. KOSTORIS), cit., p. 350 ss.

⁴⁵² Istituito con il Regolamento (UE) 2017/1939 del Consiglio relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea (EPPO) è stata pubblicata in GUUE, L 283 del 31 ottobre 2017. Per una breve trattazione sul tema del Pubblico Ministero europeo si rimanda a T. ALESCI, *La Procura europea per i reati lesivi di interessi finanziari: la proposta di regolamento tra luci e ombre*, in *Arch. Pen.*, 1, 2014, p. 1 ss.; S. ALLEGREZZA, *Pubblico ministero e azione penale: stato dell'arte e prospettive di sviluppo*, in AA.VV., *Profili del processo penale nella Costituzione europea* (a cura di M. G. COPPETTA), Torino, 2005, p. 217 ss.; S. ALLEGREZZA, A. MOSNA, *Cross-Border Criminal Evidence and the Future European Public Prosecutor. One Step Back on Mutual Recognition?*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018, p. 141 ss.; A. BERNARDI, D. NEGRI, *Rapporti tra autorità giudiziarie nazionali e organi investigativi nell'ottica della futura istituzione della Procura europea: modelli operazionali e buone pratiche nella lotta ai reati che ledono gli interessi finanziari dell'UE*, in *penalecontemporaneo.it*, 10 febbraio 2015; L. CAMALDO, *L'istituzione della Procura europea: il nuovo organo investigativo affonda le proprie radici negli ordinamenti nazionali*, in *Cass. pen.*, 2018, p. 958 ss.; P. CSONKA, A. JUSZCZAK, E. SASON, *The*

incaricata di fare indagini sulle frodi contro le finanze dell'Unione commesse in qualunque Stato membro.

Invece, quando si parla di ravvicinamento o armonizzazione delle legislazioni nazionali si fa riferimento all'attività degli Stati membri di attuazione, mediante produzione di regole interne di esecuzione, di norme fissate dall'Unione europea. Importante dottrina definisce l'armonizzazione come «il processo che conduce ad instaurare una relazione funzionale fra sistemi [...] in maniera tale che essi, all'esito del processo, risultino compatibili l'uno con l'altro e coerenti con il contesto di riferimento, armonici appunto»⁴⁵³. Tipico esempio sono le direttive che ogni singolo Stato deve recepire per potervi dare attuazione.

Establishment of the European Public Prosecutor's Office, in *Eucrim*, 3, 2017, p. 125 ss.; J.A. ESPINA RAMOS, *The Relationship Between Eurojust and the European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018; F. FALETTI, *The European Public Prosecutor's Office and the Principle of Equality*, in *Eucrim*, 1, 2017, p. 25 ss.; M. FIDELBO, *La cooperazione rafforzata come modalità d'istituzione della Procura europea*, in *Riv. dir. pen. cont.*, 3, 2016, p. 92 ss.; N. FRANSSEN, *The Future Judicial Cooperation between the EPPO and Non-Participating Member States Editorial*, in *New Journal of European Criminal Law*, 2018, p. 291 ss.; F. GIUFFRIDA, *Cross-Border Crimes and the European Public Prosecutor's Office*, in *Eucrim*, 3, 2017, p. 149 ss.; R.E. KOSTORIS, *Gli organismi centralizzati della cooperazione giudiziaria: la Procura europea*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 276 ss.; ID., *Processo penale e paradigmi europei*, cit., p. 63 ss.; L. PRESACCO, *Profili fondamentali del pubblico ministero europeo*, in *Cass. pen.*, 12, 2018, p. 4399 ss.; T. RAFARACI, *Brief Notes on the European Public Prosecutor's Office: Ideas, Project and Fulfilment*, in T. RAFARACI, R. BELFIORE (eds.), *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019, p. 157 ss.; E.P. REALE, *Defence Areas and Limits in the Investigations of the European Public Prosecutor*, in T. RAFARACI, R. BELFIORE (eds.), *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019, p. 205 ss.; S. RUGGERI, *Criminal Investigations, Interference with Fundamental Rights and Fair Trial Safeguards in the Proceedings of the European Public Prosecutor's Office. A Human Rights Law Perspective*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018, p. 201 ss.; F. SPIEZIA, *Il Pubblico Ministero Europeo e i suoi rapporti con Eurojust*, in *penalecontemporaneo.it*, 29 maggio 2018; ID., *The European Public Prosecutor's Office – How to Implement the Relations with Eurojust?*, in *Eucrim*, 2018, p. 130 ss.; A. VENEGONI, *Procura europea – EPPO*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 1176 ss.; D. VILAS ÁLVAREZ, *The Material Competence of the European Public Prosecutor's Office*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018, p. 25; M.L. WADE, *The European Public Prosecutor: Controversy Expressed in Structural Form*, in T. RAFARACI, R. BELFIORE (eds.), *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019, p. 165 ss.; S. WHITE, *Towards a Decentralized European Public Prosecutor's Office*, in *New Journal of European Criminal Law*, 1-2, 2013, p. 23 ss.; I. WIECZOREK, *The EPPO Draft Regulation Passes the First Subsidiarity Test: An Analysis and Interpretation of the European Commission's Hasty Approach to National Parliament's Subsidiarity Arguments*, in *German Law Journal*, 2015, p. 1247 ss.; V. ZAGREBELSKY, *L'istituzione del Procuratore europeo in rapporto alle esigenze dell'equo processo*, in <http://www.europeanrights.eu>, 2014, p. 54 ss.; L. CAMALDO (a cura di), *L'istituzione del Procuratore europeo e la tutela penale degli interessi finanziari dell'Unione europea*, Torino, 2014; A. ZARATE CONDE, M. PRADA RODRIGUEZ, *Transactions and "Simplified Procedures" in the Framework of the European Public Prosecutor's Office. A National Perspective*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018, p. 165.

⁴⁵³ Così, S. MANACORDA, *L'armonizzazione dei sistemi penali: una introduzione*, in AA.VV., *La giustizia penale italiana nella prospettiva internazionale*, Atti del Convegno. Courmayeur, 8-10 ottobre 1999, Milano, 2000, p. 35; si veda anche A. BERNARDI, *Strategie per l'armonizzazione dei sistemi penali europei*, in AA.VV., *Il diritto penale nella prospettiva europea* (a cura di S. CANESTRARI, L. FOFFANI), Milano, 2005, p. 407 ss.; K. TIEDEMANN, *L'europeizzazione del diritto penale*, in *Riv. it. Dir. proc. Pen.*, 1, 1998, p. 8.

L'armonizzazione è uno strumento tecnico che persegue il fine ultimo del ravvicinamento normativo degli ordinamenti tra loro diversi, il quale può essere realizzato in tre modalità diverse: ravvicinamento spontaneo, metodo induttivo e metodo deduttivo.

Il ravvicinamento spontaneo si realizza tra ordinamenti che condividono tra loro una cultura giuridica basata sulle stesse tradizioni storiche o filosofiche. Essendo basata su una comunanza di principi condivisi tra gli ordinamenti, la convergenza normativa avviene in modo naturale, senza che vi sia alcun elemento che artificialmente operi un'armonizzazione.

Il metodo induttivo ridisegna la gerarchia delle fonti di un ordinamento subordinando le norme nazionali alle norme sovranazionali, quali ad esempio le direttive dell'Unione europea. In tal caso, attraverso il recepimento della normativa sovranazionale, gli ordinamenti statuali realizzano una armonizzazione normativa indotta ed obbligatoria, ma pur sempre compatibile con il proprio sistema. Tipico esempio di armonizzazione indotta è il processo normativo del Consiglio d'Europa: le garanzie individuate dalla Convenzione europea dei diritti dell'uomo hanno introdotto nuovi obblighi in capo ai singoli Stati che l'hanno ratificata, generando un continuo dialogo tra gli ordinamenti statuali, i giudici nazionali e la Corte europea dei diritti dell'uomo, volto a determinare i principi e le garanzie fondamentali comuni⁴⁵⁴.

Il metodo deduttivo – *alias* armonizzazione dedotta – si realizza attraverso l'unificazione di uno specifico settore normativo che prevede la creazione a livello sovranazionale di un gruppo di norme condivise. Molto spesso le norme nascono per regolare una determinata materia, ma ampliano la propria portata fino a ricomprendere anche altri settori⁴⁵⁵.

Originariamente tra il mutuo riconoscimento e l'armonizzazione vi era una netta contrapposizione. Appena formulata, l'armonizzazione normativa era avvertita come strumento di compressione della sovranità statale poiché richiedeva a ogni Paese membro di adeguarsi alle decisioni provenienti dall'Unione europea; invece, il mutuo riconoscimento manifestava una maggior flessibilità in quanto strumento “alla pari” perché consentiva agli Stati membri di non mutare le regole interne e di recepire singoli atti giudiziari prodotti dagli altri Stati, di cui si presumeva si avesse fiducia. In base a ciò, si riteneva di poter fare a meno dell'armonizzazione ove era possibile applicare il mutuo riconoscimento⁴⁵⁶.

⁴⁵⁴ In tal senso S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), cit., p. 703.

⁴⁵⁵ Sul tema si veda anche S. MANACORDA, *L'armonizzazione dei sistemi penali: una introduzione*, in AA.VV., *La giustizia penale italiana nella prospettiva internazionale*, cit., p. 48. L'autrice afferma che l'armonizzazione dedotta è «il frutto della creazione di micro-sistemi normativi o istituti penalistici totalmente unificati su scala universale o regionale che recano, per propagazione, esigenze di ulteriori ravvicinamenti normativi. Se armonizzazione e unificazione presentano, sia sul piano semantico che sul piano delle logiche politico-giuridiche, una profonda divergenza, ascrivibile rispettivamente all'esistenza o al difetto di un “margine nazionale di adattamento”, vengono comunque a crearsi profonde intersezioni tra l'una e l'altra. In particolare, regole unitarie sovraordinate al diritto interno vengono a costituire, su un piano prioritariamente normativo o in un'ottica di tipo culturale, punti di riferimento indefettibili per i legislatori nazionali che devono quindi convergere verso *standards* comuni». A proposito si leggano le osservazioni di C. SOTIS, *La perspective d'un droit pénal communautaire*, in AA.VV., *L'intégration pénale indirecte: Interactions entre droit pénal et coopération judiciaire au sein de l'Union européenne* (a cura di G. GIUDICELLI-DELAGE, D. MANACORDA), Paris, 2006, p. 263 ss.

⁴⁵⁶ Cfr., O. MAZZA, *Il principio del mutuo riconoscimento nella giustizia penale. La mancata armonizzazione e il mito taumaturgico della giurisprudenza europea*, in *Riv. dir. proc.*, 2, 2009, p. 393 ss., secondo il quale «Ci si è resi conto che se a livello teorico il reciproco riconoscimento postula

In realtà, seppur in maniera più blanda rispetto all'applicazione di un più forte modello di armonizzazione, il mutuo riconoscimento senza una preventiva armonizzazione normativa poteva condurre ad una invasione e sensibile compressione della sovranità statale. Questo perché il giudice interno dovrebbe recepire o eseguire una decisione giudiziaria proveniente da un altro Stato confezionata seguendo il criterio della *lex loci*, seguendo cioè le regole del Paese di esecuzione, le quali possono ampiamente divergere rispetto alle regole interne.

Ciò portava ad un incredibile paradosso: lo stesso atto che, se acquisito a livello interno sarebbe vietato, dovrebbe essere ammesso e considerato valido qualora provenga dall'estero. Ad esempio, in Italia nell'ambito di un procedimento italiano, qualora venga eseguito un interrogatorio da parte dell'ufficio del Pubblico Ministero senza il rispetto dei diritti di difesa, non ci si potrebbe avvalere del risultato in quanto l'atto sarebbe inutilizzabile; invece, qualora l'interrogatorio – compiuto senza le garanzie per l'interrogato, perché non previste dallo Stato di esecuzione – venga eseguito all'estero e recepito in Italia, il prodotto risulterebbe a tutti gli effetti utilizzabile in quanto assunto seguendo le regole del Paese di esecuzione. In pratica, qualora si accolga il mutuo riconoscimento senza una preventiva armonizzazione, si pone il rischio che una «prova illegittima diventi utilizzabile solo perché è battezzata come 'europea'»⁴⁵⁷.

Tuttavia, col tempo e con il difficile percorso affrontato dalla decisione quadro 2002/584/GAI relativa al mandato di arresto europeo, si arriva alla piena consapevolezza che il mutuo riconoscimento non si pone in netta antitesi all'armonizzazione, ma anzi la completa, eliminandone, così, la dicotomia.

Questa tesi nasce da una evidente necessità: il mutuo riconoscimento è davvero efficace solo se tra gli Stati membri vi sia una reciproca fiducia; la reciproca fiducia vi è solo se sono presenti sufficienti caratteri di omogeneità almeno con riguardo a un insieme di norme minime. Questo insieme di norme minime comuni possono esser efficacemente garantite soprattutto con un approccio verticale, perché il vero elemento che fa la differenza è la possibilità di introdurre norme comuni stabilite a livello centrale e poi applicate in tutti gli Stati membri. La conseguenza è, allora, che il mutuo riconoscimento non può fare a meno dell'armonizzazione. Ma vi è di più: il mutuo riconoscimento, per essere efficace ed effettivo, deve presupporre un alto grado di armonizzazione⁴⁵⁸.

l'armonizzazione, in pratica tale principio si presta ad essere impiegato in modo altrettanto efficace come succedaneo dell'armonizzazione stessa, sterilizzando il problema delle diversità esistenti fra i singoli ordinamenti degli Stati membri». V., inoltre, V. MITSILEGAS, *EU Criminal Law*, cit., p. 117 ss.; R. E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in *Riv. it. dir. e proc. pen.*, 3, 2015, p. 1177 ss.

⁴⁵⁷ Testualmente E. AMODIO, *Diritto di difesa e diritto alla prova nello spazio giudiziario europeo*, in AA.VV., *Il difensore e il Pubblico Ministero europeo* (a cura di A. LANZI, F. RUGGIERI, L. CAMALDO), Padova, 2002, p. 107; Sul tema si veda anche L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 15.

⁴⁵⁸ J.R. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea*, (a cura di R.E. KOSTORIS), cit., p. 351 ss.; M. BARGIS, *La cooperazione giudiziaria penale nell'Unione europea tra mutuo riconoscimento e armonizzazione: analisi e prospettive*, cit., p. 919 ss.; M. MARCHETTI, *Dalla Convenzione di assistenza giudiziaria in materia penale dell'Unione europea al mandato europeo di ricerca delle prove e all'ordine di indagine penale*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), cit., p. 135 ss.; S. SIRACUSANO, *Tra mutuo riconoscimento e armonizzazione preventiva: quali prospettive per la circolazione della prova dichiarativa nell'ambito dell'U.E.?*, cit., p. 1 ss.

Tale impostazione, a ben vedere, è già prevista dall'art. 82, par. 2, TFUE, il quale recita: «Laddove necessario per facilitare il riconoscimento reciproco delle sentenze e delle decisioni giudiziarie e la cooperazione di polizia e giudiziaria nelle materie penali aventi dimensione transnazionale, il Parlamento europeo e il Consiglio possono stabilire norme minime deliberando mediante direttive secondo la procedura legislativa ordinaria. Queste tengono conto delle differenze tra le tradizioni giuridiche e gli ordinamenti giuridici degli Stati membri». È lo stesso Trattato sul funzionamento dell'Unione europea a concepire una cooperazione giudiziaria in materia penale irrealizzabile senza un'armonizzazione normativa funzionale ad una piena applicazione del principio del mutuo riconoscimento.

La forza dell'armonizzazione sta nel riuscire a far compiere un salto di qualità al mutuo riconoscimento, poiché è con essa che la fiducia reciproca da presunta diventa effettiva, riuscendo a garantire la piena applicazione degli strumenti basati sul mutuo riconoscimento. È necessario, quindi, perseguire l'obiettivo di avvicinare i sistemi penali e giudiziari degli Stati membri dell'Unione europea, individuando almeno i principi comuni sul piano processuale che consentano la tenuta della reciproca fiducia, la quale, altrimenti, verrebbe a mancare a causa del sentimento di diffidenza che potrebbe aleggiare tra i vari Paesi dell'Unione europea, dovuta alla diversità che *in re ipsa* esiste tra i sistemi giuridici⁴⁵⁹.

L'interazione tra mutuo riconoscimento e armonizzazione normativa con metodo induttivo è, tra l'altro, virtuosa in quanto diventa l'ingrediente principale per operare una standardizzazione delle procedure, offrendo però le stesse garanzie processuali minime, poiché gli Stati possono comunque mantenere o introdurre un livello più elevato di tutela delle persone.

Su tale punto, però, occorre una riflessione. Come visto, la dottrina maggioritaria si schiera totalmente a favore dell'operatività dell'armonizzazione, essenziale per un efficace mutuo riconoscimento⁴⁶⁰. Ma altra parte della dottrina individua numerose difficoltà pratiche relative all'applicazione dell'armonizzazione, tra cui il rischio che

⁴⁵⁹ Al riguardo si veda anche O. MAZZA, *Il garantismo al tempo del giusto processo*, cit., p. 57, il quale ritiene che il mutuo riconoscimento, se non preceduto da una consistente opera di armonizzazione, rappresenta una «vera e propria finzione», poiché manifesta «una buona dose di ipocrisia e incoerenza» anche da parte degli studiosi del diritto; G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. *Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), cit., p. 523 ss.; diversamente fa notare F. ROMOLI, *Il nuovo volto dell'Europa dopo il Trattato di Lisbona. Un'analisi penalistica "multilivello"*, in *Arch. Pen.*, 1, 2011, p. 166 ss., come nell'art. 82 TFUE sia evidente che la cooperazione giudiziaria in materia penale «è fondata» sul principio del mutuo riconoscimento delle sentenze e delle decisioni giudiziarie, mentre più semplicemente «include» il ravvicinamento delle disposizioni legislative e regolamentari degli Stati membri (che già l'art. 67 TFUE in via generale permette solo «se necessario»). Per rafforzare tale pensiero, l'Autore osserva inoltre che mentre il mutuo riconoscimento è ammesso senza alcun limite di materia, l'art. 83 TFUE riduce l'applicazione del ravvicinamento delle legislazioni nazionali a specifiche «sfere di criminalità» ed in base a determinati presupposti.

⁴⁶⁰ In tale direzione va anche la Comunicazione al Consiglio e al Parlamento europeo sul reciproco riconoscimento delle decisioni giudiziarie in materia penale e il rafforzamento della reciproca fiducia tra Stati membri [SEC (2005) 641, par. 19] ove il Consiglio afferma che «le prime applicazioni del principio di reciproco riconoscimento, in particolare con il mandato d'arresto europeo, hanno fatto emergere una serie di difficoltà che potrebbero essere in parte risolte con l'adozione a livello dell'Unione, di misure legislative d'armonizzazione. Queste ultime possono articolarsi in due direzioni: da un lato assicurarsi che le decisioni di giustizia che costituiscono l'oggetto del reciproco riconoscimento rispondano a *standard* elevati in termini di garanzie dei diritti personali, dall'altro assicurarsi che i giudici che hanno pronunciato tali decisioni fossero effettivamente nelle condizioni migliori per poterlo fare».

l'armonizzazione normativa comporti un abbassamento degli *standard* di garanzia e di tutela dovuto al fatto che un numero importante di Stati membri ancora deve implementare i livelli minimi di garanzia e di tutela richiesti⁴⁶¹. Tuttavia, non va dimenticato che, secondo l'art. 82, par. 2, ultimo periodo, TFUE, l'individuazione di norme minime di garanzia non impedisce agli Stati membri di mantenere o introdurre norme che garantiscano una tutela delle persone più elevata. Va poi ricordato che, qualora alcuni Stati non abbiano adottato i livelli minimi, saranno comunque obbligati ad aumentare di fatto gli *standard* dei diritti dei cittadini di quel determinato Stato.

Ulteriore beneficio che deriva dall'armonizzazione della normativa degli Stati membri, oltre a rendere efficiente il sensibile settore della cooperazione giudiziaria, è incentivare una virtuosa cultura dei diritti fondamentali nell'Unione europea. Infatti, l'armonizzazione ha come costante valore di riferimento il rispetto dei diritti contenuti nella Carta dei diritti fondamentali dell'Unione europea e nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali⁴⁶².

Si può, quindi, concludere affermando che oltre ad essere un obiettivo, l'armonizzazione è prima di tutto uno strumento per raggiungere un fine ultimo più nobile, maggiormente meritevole di attenzione: consentire di accettare liberamente e più facilmente le decisioni raggiunte da un altro Stato, favorendo una ragionevole durata.

Riassumendo, si può ritenere che mutuo riconoscimento, libera circolazione e armonizzazione non sono altro che tre elementi caratteristici dello stesso fenomeno: il mutuo riconoscimento serve a garantire la libera circolazione delle decisioni giudiziarie, perché è solo con tale principio che la libera circolazione può essere effettiva; ma, per poter operare correttamente, il mutuo riconoscimento ha bisogno di una preventiva armonizzazione indotta della normativa compiuta dall'Unione europea, gettando così le basi per un minimo comune denominatore tra le diverse normative nazionali e facilitando il recepimento degli atti formati in un altro Stato all'interno di uno Stato membro.

10. L'inclusione del principio del mutuo riconoscimento nel Codice di procedura penale italiano. Il titolo I-bis del Libro XI del Codice di rito

Il d. lgs. 3 ottobre 2017, n. 149⁴⁶³, concernente “disposizioni di modifica del Libro XI del Codice di procedura penale in materia di rapporti giurisdizionali con autorità straniera”, all'art. 3 ha introdotto il nuovo titolo I-bis al libro XI, con il quale si individuano i “principi generali del mutuo riconoscimento delle decisioni e dei

⁴⁶¹ In tal senso R. BELFIORE, *La prova penale “raccolta” all'estero*, Roma, 2014, p. 194. L'Autrice continua osservando che «la dottrina ha evidenziato che, mentre nel mercato comune i possibili effetti deteriori del ricorso al principio del mutuo riconoscimento – la caduta verso il basso dei livelli di qualità dei prodotti e dei servizi – sono in grado di essere arginati dal consumatore, il quale può influire attivamente sul mercato mediante la sua scelta di acquisto secondo le regole della libera concorrenza, nell'ambito della cooperazione giudiziaria penale, invece, rispetto agli effetti deteriori della liberalizzazione della circolazione delle decisioni giudiziarie – l'abbassamento degli standard di garanzia e tutela intorno al minimo comune denominatore – non vi è alcun controbilanciamento: l'individuo è, nelle procedure di cooperazione, soggetto passivo».

⁴⁶² Sul tema, si veda S. NEGRI, *L'incidenza della convenzione europea dei diritti dell'uomo sulla cooperazione giudiziaria penale nell'Unione europea*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), cit., p. 55 ss.; S. CAMPAILLA, *La “circolazione” giudiziaria europea dopo Lisbona*, in *Proc. pen. e giust.*, 5, 2011, p. 90 ss.

⁴⁶³ In G.U. 16 ottobre 2017, n. 242.

provvedimenti giudiziari tra gli Stati membri dell'Unione europea", in attuazione dell'art. 4 comma 1, lettera f) della legge delega 21 luglio 2016, n. 149.

L'obiettivo del nuovo titolo è rafforzare la cooperazione giudiziaria in materia penale tra l'Italia e gli altri Paesi dell'Unione europea attraverso l'esplicita previsione codicistica del principio del mutuo riconoscimento e dei relativi corollari che lo compongono, individuando una disciplina organica.

La scelta del legislatore di introdurre nel Codice di procedura penale il principio del mutuo riconoscimento, già previsto nel diritto dell'Unione europea, ha una portata dirompente: il legislatore ha fatto sì che il principio sia divenuto un vero e proprio pilastro del sistema e non «una semplice regola puntuale di singoli atti europei applicabili»⁴⁶⁴. Tale innesto non ha una mera valenza simbolica, ma assume una funzione «pedagogica», poiché guida l'interprete ed il legislatore tra i criteri ispiratori delle disposizioni del diritto dell'Unione europea già emanate o di futura emanazione.

Del titolo I-*bis* fanno parte nove articoli (dall'art. 696-*bis* all'art. 696-*decies* c.p.p.), i quali descrivono la disciplina e le caratteristiche generali del mutuo riconoscimento vevoli nei rapporti tra Stato italiano e altri Stati membri dell'Unione europea. Essi creano un sistema – o “binario” – parallelo a quello della classica mutua assistenza giudiziaria.

Scopo di tali norme è quello di individuare i criteri guida ispiratori delle disposizioni del diritto dell'Unione europea utili per il legislatore e per gli interpreti che operano con gli strumenti della cooperazione giudiziaria in materia penale nell'ambito dell'Unione europea, ottenendo effetti benefici quale rapidità ed efficacia.

L'art. 696-*bis* c.p.p., norma di apertura del nuovo titolo, positivizza il principio del mutuo riconoscimento «disciplinato dalle norme del presente titolo e dalle altre disposizioni di legge attuative del diritto dell'Unione europea».

Il principio del mutuo riconoscimento, così come formulato, consente alle decisioni e ai provvedimenti giudiziari «emessi dalle competenti autorità degli altri Stati membri» di poter essere riconosciuti ed eseguiti all'interno dello Stato italiano, così come «l'autorità giudiziaria italiana può richiedere alle competenti autorità degli altri Stati membri l'esecuzione dei propri provvedimenti e decisioni»⁴⁶⁵.

In tal modo, si permette all'autorità giudiziaria di poter riconoscere ed eseguire le decisioni e i provvedimenti giudiziari degli altri Stati membri senza sindacarne le ragioni di merito, eccetto nel caso di mancato rispetto dei principi fondamentali dell'ordinamento giuridico dello Stato e delle garanzie dei diritti di difesa ed individuali dell'imputato o del condannato, così come sancito dall'art. 696-*ter* c.p.p.

Non possono esser lesi i diritti fondamentali della persona riconosciuti dall'art. 6 TUE e i diritti, le libertà e i principi della Carta dei diritti fondamentali dell'Unione europea così come interpretati dalla Corte di giustizia dell'Unione europea, nonché i diritti fondamentali garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, così come interpretati dalla Corte europea dei diritti dell'uomo.

Meno agevole, invece, è l'individuazione dei principi fondamentali dell'ordinamento giuridico dello Stato, i quali, se violati, precludono il riconoscimento delle decisioni straniere in Italia. *Ictu oculi*, si potrebbe sostenere che i principi fondamentali dell'ordinamento giuridico dello Stato cui fa riferimento l'art. 696-*ter* c.p.p. siano i

⁴⁶⁴ Sul punto, si legga E. SELVAGGI, *Quel “restyling” che facilita la ricerca di chi è latitante*, in *Guida al diritto*, *Il Sole 24ore*, 45, 4 novembre 2017, p. 66 ss.

⁴⁶⁵ Così l'art. 696-*bis* c.p.p.

principi fondamentali della Costituzione, ossia il rispetto dei primi dodici articoli di essa. Senonché potrebbero essere inseriti nel novero anche gli altri principi costituzionali: in particolar modo, il riferimento è agli articoli 24, 25, 27, 102 e 111 Cost., ma anche all'art. 15 Cost. sull'inviolabilità della libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione, stella polare che deve guidare l'interprete e l'operatore del diritto soprattutto quando si avvicina al delicato tema delle intercettazioni. Infine, vanno menzionati l'art. 13 Cost. sull'inviolabilità della libertà personale e l'art. 14 Cost. sull'inviolabilità del domicilio, nonché la dignità umana intesa non come monade, ma quale premessa dei diritti fondamentali⁴⁶⁶ e sintesi di tutti i principi e diritti fondamentali⁴⁶⁷.

A ben vedere, molti principi di indiscussa rilevanza per l'ordinamento italiano sono già sanciti dal Trattato sull'Unione europea o nella Carta dei diritti dell'Uomo. Si pensi, ad esempio, al diritto ad un giudice terzo ed imparziale, il diritto a controinterrogare i testi d'accusa, il diritto a conoscere in maniera completa ed analitica la contestazione formulata, il diritto al contraddittorio. Possono, inoltre, dirsi espressione di principi fondamentali le regole nazionali che salvaguardano i principi generali sanciti dalla CEDU e dalla Carta di Nizza.

Come osservato in precedenza, il vero banco di prova consiste nell'individuare un equilibrio tra la reciproca fiducia ed il sistema dei diritti fondamentali sanciti nella Carta dei diritti fondamentali dell'Unione europea, basati sulla dignità umana, alla luce del principio del primato del diritto dell'Unione europea⁴⁶⁸.

Le procedure basate sul principio del mutuo riconoscimento risultanti dalla lettura sistematica delle norme codicistiche sono molto snelle e semplificate. Gli articoli di riferimento sono, in particolare, l'art. 696-*quater* c.p.p. recante la disciplina relativa alle modalità di trasmissione delle decisioni giudiziarie e l'art. 696-*octies* c.p.p. rubricato

⁴⁶⁶ Così, P. HÄBERLE, *Le libertà fondamentali nello Stato costituzionale*, (1983), trad. it., Roma, 1993, p. 177; D. MESSINEO, *La garanzia del "contenuto essenziale" dei diritti fondamentali. Dalla tutela della dignità umana ai livelli essenziali delle prestazioni*, Torino, 2012, p. 144; G. SILVESTRI, *L'individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale ASPP – Salerno, 25-27 ottobre 2018* (a cura di L. KALB), Milano, 2019, p. 31. Sul concetto di dignità umana, P. DE SENA, *Dignità umana in senso oggettivo e diritto internazionale*, in *Diritti umani e diritto internazionale*, 3, 2017, p. 573 ss.; A. DI STASI, *Human dignity as a normative concept: "dialogue" between European Courts (ECtHR and CJEU)?*, in P. PINTO DE ALBUQUERQUE, K. WOJTYCZEK (eds.), *Judicial power in a globalized world. Liber amicorum Vincent De Gaetano*, Cham, 2019, pp. 115-130; A. RUGGERI, *La dignità dell'uomo e il diritto di avere diritti (profili problematici e ricostruttivi)*, in *Consulta online*, 2, 2018, p. 392 ss.; G. SILVESTRI, *La dignità umana come criterio di bilanciamento dei valori costituzionali*, in *Studi in onore di Pierfrancesco Grossi*, Milano, 2012, p. 1181.

⁴⁶⁷ Cfr., Corte Cost., sentenza del 9 aprile 2013 – 9 maggio 2013, n. 85, in G.U., 15 maggio 2013, n. 20.

⁴⁶⁸ Sul tema, vi è stato un fervente confronto tra le Corti, cominciato sotto l'ombra di alcune incertezze, con attori che continuavano ad osservare le mosse degli altri protagonisti, persuasi tutti da sentimenti di diffidenza e, verosimilmente, di scetticismo nei confronti dell'altro. Il confronto, però, non si è arrestato, ed è diventato, pian piano, sempre più sincero, sino ai recenti orientamenti. È tangibile l'armonica evoluzione delle giurisprudenze nazionali, sovranazionali ed internazionali, che si avviano verso una concordanza interpretativa, verso una medesima conclusione: una tutela dei diritti umani accentuata e non comune rispetto al passato, raggiungendo un "buon equilibrio" a proposito del fondamentale principio di reciproca fiducia, aspetto cardine dello spazio di libertà, sicurezza e giustizia. Di "buon equilibrio" parla G. RAIMONDI, *Editoriale. Spazio di libertà, sicurezza e giustizia, diritti fondamentali e dialogo tra giudici*, in *Freedom, Security & Justice Review*, 2, 2019, p. 2 ss.

“modalità di esecuzione”. È possibile suddividere l’art. 696-*quater* c.p.p.⁴⁶⁹ in due parti: il comma 1 relativo alla procedura passiva e il comma 2 sulla procedura attiva.

Secondo il comma 1, la recezione delle decisioni e dei provvedimenti da riconoscere ed eseguire nel territorio dello Stato italiano avviene direttamente da parte dell’autorità giudiziaria competente. Con il termine “direttamente” il legislatore ha voluto sgomberare il campo da ogni dubbio: la recezione dell’atto si realizza con un contatto diretto tra autorità giudiziarie, con conseguente limite all’operatività del filtro politico nel potere del Ministro di giustizia, il quale assume un ruolo prevalentemente (ma non esclusivamente) tecnico-amministrativo. Inoltre, la documentazione, gli accertamenti integrativi e le ulteriori informazioni necessarie per l’esecuzione delle decisioni e dei provvedimenti sono anch’essi direttamente trasmessi tra le autorità giudiziarie.

Ulteriore aspetto è relativo alla competenza: l’art. 696-*quater* c.p.p. individua una non meglio specificata “autorità giudiziaria competente” (si badi bene: giudiziaria e non giurisdizionale), per cui spetterà all’interprete andare alla ricerca di volta in volta di tale autorità nel testo legislativo di riferimento.

Si potrebbe azzardare una riforma che preveda l’indicazione in via generale di un’autorità competente – o legittimata – ad eseguire tali attività già nel testo dell’art. 696-*quater* c.p.p. Potrebbe esser ritenuta competente – *rectius* legittimata – la Procura della Repubblica presso il Tribunale del capoluogo del distretto di Corte d’Appello del luogo in cui l’atto o gli atti dovranno essere compiuti e, in via sussidiaria e residuale, la Procura della Repubblica presso il Tribunale di Roma. Tale scelta, infatti, risulta essere più funzionale, efficace, effettiva e sicuramente garantisce una maggior speditezza nell’esecuzione delle sentenze e dei provvedimenti.

In realtà, vista la generale portata del titolo, e volendo esser garantisti, l’autorità giudiziaria competente, più che l’organo inquirente/requirente, dovrebbe essere un giudice che porta con sé delle caratteristiche di naturalità, terzietà e imparzialità. Quindi, probabilmente, competente dovrebbe essere il Tribunale del capoluogo del distretto di Corte d’appello del luogo in cui l’atto o gli atti dovranno esser compiuti e, in via residuale, il Tribunale di Roma. Ciò, però, dovrebbe prevedere un coordinamento ed una sistematizzazione con le altre fonti relative agli strumenti di mutuo riconoscimento.

Ulteriore possibilità potrebbe esser quella di individuare di volta in volta l’autorità giudiziaria competente, in base all’attività da compiere e al caso concreto, ma tale teoria aprirebbe a una discrezionalità eccessiva e del tutto in contrasto con i principi costituzionali ed europei. Tra l’altro, bisognerebbe capire chi abbia tale potere di individuazione. Per questi motivi la teoria sembrerebbe da rigettare.

Se così è, i rilievi da compiere sono due: il legislatore poteva esplicitamente disciplinare ciò all’interno del Codice di procedura penale, evitando di far compiere all’interprete una “caccia alla norma” spesso difficoltosa. Inoltre, destano non poche perplessità la legittimazione del Procuratore della Repubblica, a causa delle inferiori garanzie che tale ufficio porta con sé, sicuramente bilanciate da un’assicurazione di maggior celerità, rispetto a un giudice.

Bisogna, quindi, capire se si è disposti a sacrificare sull’altare della celerità delle procedure di cooperazione giudiziaria un fascio di garanzie che ontologicamente sono valutate dal giudice, ovvero se nonostante tali disposizioni, queste siano recuperabili nelle sedi previste per le impugnazioni, così come sembra consenta l’art. 696-*novies* c.p.p. In

⁴⁶⁹ Per un commento all’art. 696-*quater* c.p.p., A. MANGIARACINA, sub *Art. 696-quater c.p.p.*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 32 ss.

virtù di una generica uniformazione, appare questa la scelta attualmente ritenuta più opportuna dal legislatore.

Il comma 2 dell'art. 696-*quater* c.p.p. disciplina la trasmissione diretta delle decisioni e dei provvedimenti da riconoscere ed eseguire da parte delle competenti autorità giudiziarie di un altro Stato membro, previa comunicazione al Ministro della giustizia nei casi e nei modi previsti dalla legge. La comunicazione è necessaria anche ai fini dell'esercizio dei poteri che espressamente sono previsti in capo al Ministro della giustizia dall'art. 696-*sexies* c.p.p.⁴⁷⁰

Da una parte, per le procedure passive si stabilisce che «il Ministro della giustizia, nei casi e nei modi previsti dalla legge, garantisc[a] l'osservanza delle condizioni eventualmente poste in casi particolari dall'autorità giudiziaria dello Stato membro per dare esecuzione alle decisioni giudiziarie di cui è stato chiesto il riconoscimento, sempre che tali condizioni non contrastino con i principi fondamentali dell'ordinamento giuridico dello Stato»; dall'altra, per le procedure attive, si sancisce che lo stesso «verifi[chi] l'osservanza delle condizioni poste dall'autorità giudiziaria italiana per l'esecuzione delle decisioni e dei provvedimenti nel territorio di altro Stato membro».

Al Ministro della giustizia, quindi, sembra sia stato sottratto del tutto qualsiasi potere di valutazione preventiva avente come fine la verifica dell'eseguibilità della decisione straniera in Italia. Il ruolo del Ministro, però, non è assolutamente marginale, anche se è ridotto a una mera funzione di garanzia della corretta osservanza delle procedure affinché non contrastino con i principi fondamentali dell'ordinamento italiano.

L'interessante tema merita un breve approfondimento. In via preliminare, si è detto che al Ministro della giustizia è sottratta qualsiasi valutazione preventiva sulla richiesta di riconoscimento al fine di verificare l'eseguibilità della decisione perché è previsto che le decisioni giudiziarie da eseguirsi nel territorio dello Stato italiano possano essere trasmesse direttamente all'autorità giudiziaria territorialmente competente per l'esecuzione e che l'autorità giudiziaria italiana possa trasmettere direttamente allo Stato di esecuzione le decisioni delle quali si chiede il riconoscimento.

Ciò in considerazione del fatto che il controllo sul rispetto dei principi fondamentali dell'ordinamento giuridico dello Stato è stato preventivamente effettuato, in ragione della disciplina generale individuata dal diritto dell'Unione europea. Non va dimenticato che la reciproca fiducia presume rispettati i diritti fondamentali da parte degli altri Stati membri, con la conseguente impossibilità di esigere un livello di tutela nazionale più elevato di quello garantito dal diritto dell'Unione e, salvo casi eccezionali, di verificare se lo Stato membro sia effettivamente rispettoso dei diritti fondamentali dell'Unione europea, tant'è che solo a seguito della constatazione dell'esistenza di seri e comprovati motivi di ritenere che nell'altro Stato non siano garantiti i diritti fondamentali, si potrà rifiutare l'esecuzione dell'atto⁴⁷¹.

Il Ministro, però, conserverebbe un ruolo amministrativo. Sarebbe un organo che riceve e trasmette gli atti e che, eventualmente, li traduce. Senonché, l'articolo 696-*sexies* c.p.p. sembrerebbe far riemergere in capo ad egli importanti poteri divergenti in base alla procedura seguita (attiva o passiva).

Il comma 1 disciplina le ipotesi relative alle procedure passive. In tali procedure il Ministro acquista un ruolo di garanzia del rispetto delle condizioni poste in casi particolari

⁴⁷⁰ Per un commento, A. MANGIARACINA, sub *Art. 696-sexies c.p.p.*, in AA.VV., *Cooperazione giudiziaria penale*, (a cura di A. MARANDOLA), Milano, 2018, p. 42 ss.

⁴⁷¹ Cfr., Corte di giustizia, Grande Sezione, sentenza del 15 ottobre 2019, *Dumitru-Tudor Dorobantu*, causa C-128/18.

dall'autorità giudiziaria di un altro Stato in capo alle autorità giudiziarie italiane che dovranno dare esecuzione alle decisioni giudiziarie di cui è stato chiesto il riconoscimento, purché tali condizioni non siano in contrasto con i principi fondamentali dell'ordinamento giuridico dello Stato italiano.

Le modalità con cui il Ministro dovrà esercitare tali poteri saranno individuate da non meglio specificate leggi, alle quali la norma rimanda. Ora, se non si vuole ridurre tutto a un mero potere del tutto formale, si dovrà almeno prevedere che l'autorità giudiziaria straniera trasmetta le proprie decisioni sia all'autorità giudiziaria italiana sia al Ministro.

Ciò sembra previsto proprio all'art. 696-*quater*, comma 2, c.p.p. Interessante sarà capire fino a che punto potrà spingersi il potere di garanzia del Ministro, senza ledere quella che è una caratteristica basilare del principio del mutuo riconoscimento: l'eliminazione del filtro politico. Tale potere di garanzia in capo al Ministro è riconosciuto unicamente nei casi individuati dalla legge, quindi non sempre e comunque, e soltanto quando sono state poste eventualmente delle condizioni in casi particolari dall'autorità giudiziaria dello Stato di emissione.

Il comma 2 regola, invece, le procedure attive. Qui il Ministro della giustizia acquista un potere di verifica delle condizioni poste dall'autorità giudiziaria italiana per l'esecuzione delle decisioni e dei provvedimenti nel territorio di un altro Stato membro. L'autorità giudiziaria italiana può porre sempre delle condizioni per l'esecuzione della decisione; l'autorità giudiziaria straniera, nell'eseguire la decisione o il provvedimento, dovrà rispettare tali condizioni; una volta eseguito il provvedimento o la decisione, il Ministro della giustizia dovrà verificare *ex post* il rispetto delle sole condizioni poste, e non dovrà spingersi sino a compiere una verifica generale sull'intero atto che entri nel merito.

Il comma 2, a differenza del comma 1, non prevede l'inciso "nei casi e nei modi previsti dalla legge". Il motivo sembra abbastanza evidente: se specularmente nella procedura passiva questi debba garantire l'osservanza delle particolari condizioni poste da una autorità giudiziaria di un altro Stato membro, è ovvio che ogni volta che sia prevista l'osservanza di condizioni poste dall'autorità giudiziaria italiana, per questioni di garanzia, sia compiuta una verifica sul rispetto di queste da parte del Ministro.

Ci si chiede, però, perché il Ministro della giustizia dovrebbe verificare il rispetto delle condizioni (di tutte le condizioni, non solo di quelle particolari) poste dall'autorità giudiziaria italiana, se si tratta di strumenti che operano secondo il principio del mutuo riconoscimento, e quindi basati su una reciproca fiducia tra Stati membri. Sembra, pertanto, che la norma voglia in qualche modo riaffermare la potestà sovrana statale attraverso un precipitato storico che ingessa – seppur parzialmente – la procedura.

In conclusione, il Ministro della giustizia acquista una nuova funzione. I poteri del Ministro della giustizia non hanno unicamente aspetti positivi ma nascondono anche ombre: il rischio è che si irrigidiscano le procedure tra Stati membri, laddove l'obiettivo dell'Unione europea è sempre stato quello di creare procedure snelle, veloci ed efficienti.

L'art. 696-*novies* c.p.p. disciplina l'istituto dell'impugnazione. Le decisioni sul riconoscimento e l'esecuzione di un provvedimento emesso dall'autorità giudiziaria di altro Stato membro sono impugnabili nei casi e con i mezzi previsti dalla legge. Invece, avverso le sentenze e i provvedimenti sulla libertà personale è ammesso il ricorso per Cassazione per violazione di legge. Sono, infine, ammesse le impugnazioni per motivi di merito solo se espressamente previsto, in linea con quanto indicato dall'art. 696-*quinquies* c.p.p.

Inoltre, ai terzi è assicurata la partecipazione al procedimento di riconoscimento con le forme e le garanzie che la legge prevede per i procedimenti analoghi già regolati dall'ordinamento interno.

Il riconoscimento e l'esecuzione delle decisioni e dei provvedimenti giudiziari degli altri Stati membri devono avvenire, secondo l'art. 696-*octies* c.p.p., «senza ritardo e con modalità idonee ad assicurare la tempestività e l'efficacia» della procedura. A tale *ratio* risponde anche il comma 2 del medesimo articolo, secondo cui «all'esecuzione delle decisioni e dei provvedimenti giudiziari al cui riconoscimento l'interessato ha prestato il consenso si provvede senza formalità, nel rispetto dei diritti fondamentali della persona». L'articolo, però, non ribadisce il necessario rispetto dei diritti fondamentali dell'ordinamento giuridico statale, ma si riferisce unicamente ai diritti della persona. I diritti processuali sono comunque garantiti in virtù dell'applicabilità in via generale dell'art. 696-*ter* c.p.p. che esplicitamente dispone il rispetto in ogni caso dei principi fondamentali dell'ordinamento giuridico in ogni fase e per ogni atto relativo al mutuo riconoscimento. Non è mai possibile riconoscere decisioni o eseguire provvedimenti che possano ledere i diritti fondamentali della persona, anche se vi è il consenso dell'interessato stesso.

La disciplina sul mutuo riconoscimento è applicata anche alle decisioni relative alla responsabilità degli enti da reato. L'art. 696-*septies* c.p.p., rubricato “mutuo riconoscimento e responsabilità da reato degli enti”, sancisce che «in materia di mutuo riconoscimento delle decisioni giudiziarie riguardanti la responsabilità da reato degli enti, nei rapporti con gli Stati membri dell'Unione europea, si osservano le norme di questo titolo nonché quelle contenute in altre disposizioni di legge attuative del diritto dell'Unione europea». Qui si rilevano criticità del tutto analoghe a quelle dell'art. 696-*bis* c.p.p. che verrà analizzato nel prossimo paragrafo⁴⁷².

⁴⁷² La norma porta con sé un ulteriore elemento di non poco conto: viene inserito esplicitamente nel Codice di procedura penale una norma relativa alla responsabilità dell'ente da reato. Ora, il d. lgs. 8 giugno 2001, n. 231 qualifica la responsabilità di tali enti come “amministrativa”, ma la dottrina è praticamente unanime nel ritenerla una forma di responsabilità di fatto penale. La scelta del legislatore di qualificare come amministrativa tale responsabilità è in fondo coerente con il principio individualistico “*societas delinquere non potest*”, secondo cui le persone giuridiche e, più in generale, gli enti collettivi anche non riconosciuti, non possono commettere reati, e pertanto, non potrebbero essere sanzionati con i classici strumenti del diritto penale. Il principio è deducibile anche dall'art. 27 Cost. secondo cui la responsabilità penale è personale e le pene devono avere una finalità rieducativa. In tale caso, ci si chiede come faccia una pena a rieducare un ente collettivo che, *in re ipsa*, non ha una coscienza e una volontà, che non è “entità pensante”. Quindi, molti sono gli ostacoli alla responsabilità penale dell'ente: l'ente risponderebbe per condotta altrui, ma la responsabilità deve essere personale; l'ente non è capace di un atteggiamento volitivo, per cui si lederebbe il principio di colpevolezza e non sarebbe applicabile una sanzione finalisticamente orientata alla rieducazione; l'ente non è un individuo, una persona fisica, per cui si lederebbe il principio individualistico. Senonché, il legislatore ha avvertito la necessità di superare i problemi nati dall'applicazione di tali principi, siccome alcune tra le più gravi forme di criminalità di tipo economico si manifestano proprio nelle società e negli enti. Infatti, alla teoria sinora esposta, si contrappone la teoria organicistica della persona giuridica che riconosce soggettività all'ente poiché vi sarebbe un rapporto di rappresentanza organica tra l'ente e le persone fisiche che ne determinano la volontà e l'azione, con la conseguenza che le attività delle persone fisiche diventano automaticamente imputabili all'ente. Il problema, però, rimane aperto comunque sotto il profilo dell'elemento della colpevolezza, in quanto resta alto il rischio di riconoscere una responsabilità oggettiva. È proprio a causa di tali difficoltà che oggi è attribuita in capo all'ente una responsabilità amministrativa, ma di fatto penale. Il d. lgs. 8 giugno 2001, n. 231 introduce un nuovo modello di responsabilità per prevenire la commissione di reati all'interno degli enti collettivi da parte dei loro organi o dei loro sottoposti. L'impressione, allora, è che il legislatore abbia voluto solo formalmente definire amministrativa una responsabilità che di fatto è penale. Infatti, la responsabilità dell'ente è strettamente agganciata alla commissione di un fatto di reato, ed inoltre la sede in

Orbene, è utile ricordare che questa serie di principi è di solito ricorrente negli strumenti normativi dell'Unione, per cui sembra dubbia l'effettiva utilità di inserimento all'interno del Codice di procedura penale. Probabilmente possono costituire un ulteriore mezzo di interpretazione di tali principi e delle norme sovranazionali ovvero, come fa notare importante dottrina, possono essere inseriti nella normativa di recepimento se non contemplate nel provvedimento da implementare e purché non in contrasto con il suo contenuto⁴⁷³.

11. (Segue). La formulazione del nuovo art. 696-bis c.p.p.

Si è detto che il d. lgs. 3 ottobre 2017, n. 149⁴⁷⁴, che modifica il Libro XI del Codice di procedura penale in materia di rapporti giurisdizionali con autorità straniera, introduce il nuovo art. 696-bis c.p.p., rubricato "principio del mutuo riconoscimento". Il comma 1 recita: «il principio del mutuo riconoscimento è disciplinato dalle norme del presente titolo e dalle altre disposizioni di legge attuative del diritto dell'Unione europea», mentre il comma 2 prevede che «le decisioni e i provvedimenti giudiziari emessi dalle competenti autorità degli altri Stati membri possono essere riconosciuti ed eseguiti nel territorio dello

cui è accertata tale responsabilità è quella del processo penale in quanto si instaura un *simultaneus processus*, per cui la sorte dell'ente sarà decisa dallo stesso giudice che accerterà la responsabilità penale dell'autore. Se poi si analizzano le sanzioni comminabili all'ente, si nota che queste sono di fatto sanzioni penali, se si applicano i c.d. criteri *Engel* elaborati dalla C. eur. dir. uomo, *Grande Camera*, sent. 23 novembre 1976, *Engel e altri c. Paesi Bassi*, come successivamente affinati. Ulteriore indizio a sostegno della tesi secondo cui sarebbe una responsabilità di fatto penale è proprio l'aver inserito in maniera esplicita la responsabilità dell'ente da reato all'interno del Codice di procedura penale all'art. 696-septies c.p.p., seppur solo in relazione alla materia del mutuo riconoscimento delle decisioni giudiziarie. La letteratura in tema di ente da reato è vastissima. Per un'ampia trattazione si rimanda, *ex multis*, a D. CIMADOMO, *Brevi considerazioni in tema di simultaneus processus nel "sistema 231"*, in *Riv. Pen.*, 11, 2021, p. 1012 ss.; ID., *Le modifiche in tema di responsabilità "amministrativa" degli enti derivante da reato*, in AA.VV., *La nuova disciplina dei delitti di corruzione. Profili penali e processuali* (L. 9 gennaio 2019, n. 3 c.d. "spazzacorrotti") (a cura di G. FLORA, A. MARANDOLA), Pisa, 2019, p. 157 ss.; ID., *La difesa dell'ente sottoposto a procedimento penale*, in *Proc. pen. e giust.*, 5, 2017, p. 942 ss.; F. CORDERO, *Procedura penale*, cit., p. 1327 ss.; G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, settima edizione, Bologna, 2014; p. 171 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 1079 ss.; R. GAROFOLI, *Manuale di diritto penale*, Roma, 2017, p. 377 ss.; F. BRICOLA, *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Riv. it. dir. e proc. pen.*, 1970, p. 951 ss.; M. GALLO, *Capacità penale*, in *Nov. Dig. it.*, vol. II, Torino, 1958, p. 882 ss.; G. DE VERO, *La responsabilità penale delle persone giuridiche*, in AA.VV., *Trattato di diritto penale* (diretto da C.F. GROSSO, T. PADOVANI, A. PAGLIARO), Milano, 2008; G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, Milano, 2012; G. DE SIMONE, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in *penalecontemporaneo.it*, 28 ottobre 2012; M. CERESA GASTALDO, *La responsabilità degli enti: profili di diritto processuale*, in AA.VV., *Impresa e giustizia penale: tra passato e futuro*. Atti del Convegno. Milano, 14-15 marzo 2008, Milano, 2009, p. 321 ss.; C.E. PALIERO, *Dieci anni di "corporate liability" nel sistema italiano: il paradigma imputativo nell'evoluzione della legislazione e della prassi*, in AA.VV., *D.lgs. n. 231: dieci anni di esperienze nella legislazione e nella prassi*, in *Soc.*, 2011, n. spec., p. 5 ss.; P. SFAMENI, *Responsabilità patrimoniale e vicende modificative dell'ente*, in AA.VV., *Responsabilità "penale" delle persone giuridiche* (a cura di A. GIARDA, E.M. MANCUSO, G. SPANGHER, G. VARRASO), Milano, 2007, p. 232 ss. Sull'argomento, anche, D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, Milano, 2016.

⁴⁷³ Sul tema, si legga M.R. MARCHETTI, *Cooperazione giudiziaria: innovazioni apportate e occasioni perdute*, in *Dir. pen. proc.*, 12, 2017, p. 1545 ss.

⁴⁷⁴ In G.U. 16 ottobre 2017, n. 242.

Stato; l'autorità giudiziaria può richiedere alle competenti autorità degli altri Stati membri l'esecuzione dei propri provvedimenti e decisioni».

Già dalla rubrica si evince che scopo della norma dovrebbe esser quello di individuare una definizione di mutuo riconoscimento utile all'orientamento dell'interprete e del futuro legislatore, così come inteso dagli articoli successivi. Caratteristiche fondamentali sono la diretta corrispondenza tra autorità; attenzione particolare ai diritti fondamentali dell'ordinamento; limiti al sindacato del provvedimento da eseguire.

Tuttavia, molti sono i punti problematici e oscuri della norma, relativi all'interpretazione sistematica da darne con le altre norme del codice e con le disposizioni della legge di delega.

Il punto di partenza è l'analisi dell'art.696-*bis* c.p.p. alla luce della sua legge di delega. I problemi che sorgono dal rapporto tra tali due norme sono tra i più complessi da risolvere.

La l. 21 luglio 2016, n. 149⁴⁷⁵ sulla “ratifica ed esecuzione della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea, fatta a Bruxelles il 29 maggio 2000, e delega al Governo per la sua attuazione. Delega al Governo per la riforma del libro XI del codice di procedura penale. Modifiche alle disposizioni in materia di estradizione per l'estero: termine per la consegna e durata massima delle misure coercitive” all'art. 4 dispone: « Il Governo è delegato ad adottare uno o più decreti legislativi per la riforma del libro XI del codice di procedura penale, con le modalità e nei termini previsti dal comma 2 del presente articolo e nel rispetto dei seguenti principi e criteri direttivi: [...] f) in materia di mutuo riconoscimento delle sentenze e delle altre decisioni giudiziarie nei rapporti con gli altri Stati membri dell'Unione europea, fermo restando quanto previsto dalla lettera e), ai soli fini della garanzia giurisdizionale: 1) prevedere che le decisioni giudiziarie emesse dalle competenti autorità degli altri Stati membri dell'Unione europea possano essere eseguite nel territorio dello Stato e che l'autorità giudiziaria possa richiedere alle competenti autorità degli altri Stati membri dell'Unione europea l'esecuzione di proprie decisioni in conformità al principio del mutuo riconoscimento; prevedere che altre disposizioni di legge si applichino solo se compatibili con le norme contenute nel codice di procedura penale e che, in ogni caso, l'esecuzione della decisione non pregiudichi l'osservanza degli obblighi internazionali assunti dallo Stato».

Prima facie, è chiaro l'intento del legislatore delegante di voler disciplinare nel Codice di procedura penale il principio del mutuo riconoscimento di chiaro stampo europeistico, ed è evidente la volontà di individuare una norma che indichi cosa si intenda per mutuo riconoscimento, a cosa serva, a quali risultati porti, e a quali norme rifarsi per la relativa applicazione.

Ora, ferma restando la gerarchia normativa individuata dal nuovo art. 696 c.p.p. così come riformato dal d. lgs. 3 ottobre 2017, n. 149 che, in ragione del principio di sussidiarietà, individua, nei rapporti con gli Stati membri dell'Unione europea, la preminenza delle norme del Trattato sull'Unione europea e del Trattato sul funzionamento dell'Unione europea, nonché degli atti normativi adottati in attuazione dei medesimi, e qualora tali norme manchino o non dispongano diversamente, prevede l'applicazione delle norme delle convenzioni internazionali in vigore per lo Stato e le norme di diritto internazionale generale, e solo se anche tali norme manchino o non dispongano diversamente, prevede l'applicazione delle norme del Libro XI del Codice di procedura penale, il legislatore delegante avrebbe voluto che accanto alle norme relative

⁴⁷⁵ Pubblicata in G.U. 4 agosto 2016, n.181.

al mutuo riconoscimento contenute in tale Libro XI al titolo I-*bis*, fossero applicabili anche altre norme, ma solo se compatibili con quelle contenute nel titolo appena citato. Ciò risulta dall'inciso «prevedere che le altre disposizioni di legge si applichino solo se compatibili con le norme contenute nel codice di procedura penale».

È evidente la distrazione del legislatore quando indica la compatibilità con le norme del codice inteso *tout court*, e non solo con il titolo I-*bis* o con le norme che regolano il mutuo riconoscimento all'interno del libro XI, perché essenzialmente con la lettera f) della legge delega il legislatore voleva che il principio del mutuo riconoscimento si coordinasse con le nuove norme contenute in tale nuovo titolo, non avendo alcuna intenzione di estendere il campo ad una modifica che riguardi l'intero assetto della normativa codicistica alla luce del mutuo riconoscimento, anche perché non vi sarebbe alcuna ragione per farlo.

E allora, bisogna dedurre che il legislatore volesse individuare una compatibilità tra le norme *extra codicem* che regolano la materia del mutuo riconoscimento e le norme contenute nel nuovo titolo I-*bis*. Non avrebbe senso regolare la compatibilità di disposizioni di legge non meglio individuate situate al di fuori del codice e che riguardino ogni aspetto della procedura penale con l'intero sistema processuale normato dal codice di procedura penale, poiché, si ribadisce, la lettera f) doveva limitarsi solamente a chiedere una regolamentazione in materia di mutuo riconoscimento.

Orbene, se il legislatore delegante ha voluto equiparare – giustamente – alle norme del titolo I-*bis* anche le altre disposizioni di legge, bisogna capire a quali norme *extra codicem* stia facendo riferimento. Il dubbio è che il legislatore si sia riferito non solo alle leggi ordinarie ed agli atti ad esse equiparate, ma anche alle leggi attuative del diritto dell'Unione europea, vista l'ampia formula utilizzata. Ed è questo il punto su cui probabilmente ha riflettuto il legislatore del decreto legislativo.

Infatti, l'art. 696-*bis* c.p.p. ha un senso totalmente diverso da quello prospettato dal legislatore delegante. La norma, invece di prevedere che il principio del mutuo riconoscimento venga regolato dalle norme del titolo e dalle altre disposizioni di legge in quanto con esse compatibili, dispone che il principio sia disciplinato «dalle norme del presente titolo e dalle altre disposizioni di legge attuative del diritto dell'Unione europea». Evidentemente, il legislatore del decreto legislativo ha inteso che l'espressione «altre disposizioni di legge si applichino solo se compatibili con le norme del codice di procedura penale» volesse riferirsi alle leggi attuative del diritto dell'Unione europea, evitando la disapplicazione – o l'abrogazione implicita – delle leggi precedenti la riforma non compatibili con essa.

Più coerentemente, il legislatore avrebbe dovuto formulare in tal modo la norma: «Il principio del mutuo riconoscimento è disciplinato dalle altre disposizioni di legge attuative del diritto dell'Unione europea e dalle norme del presente titolo».

12. Il principio di equivalenza e il principio di proporzionalità nel sistema dell'Unione europea

Se da una parte l'Unione europea ha dovuto individuare nel principio del mutuo riconoscimento uno degli elementi necessari per una efficace e rapida lotta alla criminalità transfrontaliera, dall'altra è andata alla ricerca di principi che controbilanciassero gli «effetti collaterali» del mutuo riconoscimento, al fine di razionalizzare la cooperazione

giudiziaria⁴⁷⁶. Tali principi sono stati individuati nel principio di equivalenza e nel principio di proporzionalità.

Punto di partenza è l'art. 6 TUE, il quale dispone che l'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea, avente lo stesso valore giuridico dei Trattati, e che tali diritti, libertà e principi sono interpretati conformemente a quanto stabilito dal Titolo VII della Carta; i diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali.

Dall'articolo si evince che l'Unione europea ha richiesto un equo bilanciamento tra gli obiettivi posti e i diritti fondamentali, in modo da evitare che gli uni siano azzerati completamente dagli altri⁴⁷⁷.

Il principio di equivalenza e il principio di proporzionalità tendono proprio a realizzare questo delicato equilibrio prospettato dall'art. 6 TUE. I principi sono disciplinati dalla Carta dei diritti fondamentali dell'Unione europea⁴⁷⁸ al titolo VII, ove sono contenute le disposizioni generali relative alla disciplina dell'interpretazione e dell'applicazione della Carta.

Il principio di equivalenza è disciplinato dagli artt. 52, commi 3 e 4 e dall'art. 53 della Carta, mentre il principio di proporzionalità è disciplinato dall'art. 52 della Carta⁴⁷⁹.

Secondo il principio di equivalenza, il diritto dell'Unione europea deve garantire che i diritti fondamentali abbiano un livello di tutela non inferiore a quello che essi ricevono dagli altri ordinamenti con cui l'Unione interagisce⁴⁸⁰: pensiamo, ad esempio, ai rapporti tra Unione europea e gli ordinamenti internazionali, o ai rapporti con gli Stati membri o ancora ai rapporti con la CEDU, ma anche ai rapporti che nascono grazie alle Convenzioni internazionali. Ovviamente, non è preclusa all'Unione la possibilità di concedere una protezione più estesa. Comunque, i diritti fondamentali vanno interpretati in armonia con le tradizioni costituzionali comuni agli altri Stati membri.

⁴⁷⁶ Sul rapporto tra mutuo riconoscimento e il principio di proporzionalità, P. SPAGNOLO, *La nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, cit. p. 1297 ss.

⁴⁷⁷ Sul tema si veda M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Riv. pen. cont.*, 4, 2015, p. 92; R. PICCIRILLO, *I profili funzionali e strutturali dell'Ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE-L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 71.

⁴⁷⁸ La Carta è stata proclamata a Strasburgo il 12 dicembre 2007 (in GUUE 14 dicembre 2007, n. C-303), e pubblicata nella sua versione consolidata in GUUE 7 giugno 2016, C-202. Il testo riprende la Carta di Nizza (in GUCE 18 dicembre 2000, C-364), adattandola al Trattato di Lisbona, per questo è anche impropriamente nota come "Carta di Nizza". Con l'entrata in vigore del Trattato di Lisbona, la Carta assume lo stesso valore giuridico dei Trattati in forza dell'art. 6, comma 1, TUE. La Carta è divisa in sette titoli: i primi sei contengono le disposizioni relative alla dignità, alla libertà, all'uguaglianza, alla solidarietà, alla cittadinanza e alla giustizia, mentre l'ultimo titolo contiene i principi per una corretta interpretazione e applicazione della Carta.

⁴⁷⁹ Per una analisi della disposizione si rinvia, *ex multis*, a S. PEERS, S. PRECHAL, *Article 52*, in AA.VV., *The EU Charter of Fundamental Rights: A Commentary* (a cura di S. PEERS, T. HARVEY, J. KENNER), Oxford, 2014, p. 1455 ss.

⁴⁸⁰ L'art. 53 della Carta dei diritti fondamentali dell'Unione europea recita: «Nessuna disposizione della presente Carta deve essere interpretata come limitativa o lesiva dei diritti dell'uomo e delle libertà fondamentali riconosciuti, nel rispettivo ambito di applicazione, dal diritto dell'Unione, dal diritto internazionale, dalle convenzioni internazionali delle quali l'Unione o tutti gli Stati membri sono parti, in particolare dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, e dalle costituzioni degli Stati membri».

La dottrina, però, rileva come spesso tale principio sia concretamente poco praticabile, riducendosi a una mera disposizione di carattere idealistico. Infatti, sono ipotizzabili situazioni in cui l'equivalenza potrebbe esser realizzata solo al costo di vanificare gli obiettivi individuati dall'Unione europea⁴⁸¹.

Invece, il principio di proporzionalità⁴⁸² individua un efficace metodo di controllo della corretta attuazione dei diritti fondamentali anche nell'ambito del processo penale⁴⁸³. Il principio funge da utile parametro per l'armonizzazione degli ordinamenti statuali grazie alla sua natura: infatti indica non solo la proporzione ma anche il metodo da seguire per realizzare un'adeguata tutela dei diritti. Questo perché da una parte opera come limite alla discrezionalità degli Stati membri nell'applicazione e nel riconoscimento dei diritti e delle libertà, dall'altra è anche un utile parametro di riferimento per la verifica della effettiva tutela di tutti i diritti fondamentali.

Il principio persegue il fine dell'effettività, dell'equità e della giustizia del caso concreto, attraverso lo sviluppo non tanto di previsioni formali, quanto di buone prassi, o attraverso una visione omnicomprensiva del fenomeno processuale⁴⁸⁴.

Il principio di proporzionalità, così come individuato dall'art. 52, comma 1 della Carta dei diritti fondamentali dell'Unione europea, oltre a individuare un primo ovvio filtro nel principio di legalità con l'inciso "limitazioni [...] previste dalla legge", impone il compimento di tre verifiche:

⁴⁸¹ Cfr. M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, cit., p. 92.

⁴⁸² Il principio di proporzionalità è di matrice europea, in particolare tedesca. Nasce in ambito pubblicistico. Considerando il fatto che la scuola tedesca è tra le più importanti espressioni della cultura giuridica continentale, la sua genesi lo rende apparentemente di facile assimilabilità da parte di tutti i Paesi europei di *civil law*. Invece, la sua elevata flessibilità soprattutto per quanto riguarda la componente argomentativa e persuasiva del metodo giuridico, lo rendono particolarmente fruibile anche dai sistemi di *common law*, per questo può esser facilmente recepito da tali ordinamenti, caratterizzati da una formazione culturale diversa. Nella procedura penale italiana, è possibile rintracciare tale principio in tema di misure cautelari all'art. 275 c.p.p. Qui, il principio di proporzionalità è utilizzato come uno dei criteri di scelta delle misure cautelari. Esso indica che la misura deve esser proporzionata al caso concreto. Ed infatti il comma 2 dispone che «ogni misura deve esser proporzionata all'entità del fatto e alla sanzione che sia stata o che si ritiene possa esser irrogata», cioè una misura, valutata *rebus sic stantibus*, non più grave di quella che proporzionalmente sarà l'eventuale sanzione che sarà irrogata, qualora il sottoposto a misura cautelare, processato, venga riconosciuto colpevole con sentenza passata in giudicato. In tal modo, il codice vuole evitare che si faccia un uso spregiudicato delle misure cautelari, facendo in modo che tale "necessaria ingiustizia" (Carrara), si trasformi in una somma ingiustizia, perdendo il connotato della necessità. Ma il principio di proporzionalità è rintracciabile anche all'art. 326 c.p.p., il quale dispone che «il pubblico ministero e la polizia giudiziaria svolgono, nell'ambito delle rispettive attribuzioni, le indagini "necessarie" per le determinazioni inerenti all'esercizio dell'azione penale». Sul tema, si legga V. GREVI, *Commento all'art. 9 l. 28/7/1984 n. 398*, in *Leg. pen.*, 1985, p. 151 ss., in particolare p. 156 e 157; M. CHIAVARIO, sub *Art. 275 c.p.p.*, in AA.VV., *Commento al nuovo codice di procedura penale* (a cura di M. CHIAVARIO), Torino, 1990, vol. 3, p. 61 e in particolare p. 62; R.E. KOSTORIS, *Diritto europeo e giustizia penale*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019, p. 13 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 464 ss.; M.A. SANDULLI, *Proporzionalità*, in *Dizionario di diritto pubblico*, V, Milano, 2006, p. 4643 ss. Più di recente, anche, G. SILVESTRI, *L'individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*, cit., p. 29 ss.

⁴⁸³ In tal senso, M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, 3-4, 2014, p. 145 ss.; M. DANIELE, *Testimony through a Live Link in the Perspective of the Right to Confront Witnesses*, in *Crim. Law Rev.*, 3, 2014, p. 196 ss.; D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, in AA.VV., *Diritti della persona e nuove sfide del processo penale* (a cura di L. KALB), Milano, 2019, p. 55 ss.

⁴⁸⁴ Così, M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, cit., p. 145.

- la limitazione del diritto fondamentale prevista da una norma UE deve perseguire “finalità di interesse generale riconosciute dall’Unione” o l’“esigenza di proteggere i diritti e le libertà altrui”;
- devono esistere fattori di compensazione capaci di “rispettare il contenuto essenziale” del diritto fondamentale;
- la limitazione deve essere strettamente “necessaria”, non esistendo alternative meno invasive per il diritto fondamentale ugualmente capaci di assicurare l’obiettivo perseguito⁴⁸⁵.

Il diritto dell’Unione europea, quindi, può comprimere i diritti fondamentali e arrivare a fissare livelli di protezione inferiori a quelli stabiliti dai vari ordinamenti e dalla CEDU solo rispettando rigorosamente questi tre parametri.

La Corte di giustizia ha utilizzato adeguatamente il principio in esame, applicando i parametri e i criteri individuati in maniera precisa a partire dalla sentenza *Digital Rights Ireland Ltd*⁴⁸⁶ dell’8 aprile 2014, con la quale ha dichiarato l’invalidità della direttiva sulla conservazione dei dati di traffico⁴⁸⁷ che consentiva di conservare una ingente quantità di dati sensibili relativi alla vita privata delle persone per un tempo irragionevolmente lungo, violando in tal modo il criterio della stretta necessità. Tutto ciò a causa della mancanza di norme che obblighino ad accertare la reale indispensabilità della conservazione per la lotta alla criminalità.

Ed ecco che si manifesta in tutta la sua portata il bilanciamento tra principi, esigenze ed obiettivi. La Corte, nel ribadire gli *standards* di tutela individuati dalla Corte europea dei diritti dell’Uomo nella decisione *Marper c. Regno Unito*⁴⁸⁸, ha ravvisato la violazione degli articoli 7, 8 e 11 della Carta relativi al diritto al rispetto della vita privata, della protezione dei dati di carattere personale e di libertà di espressione.

Alle stesse conclusioni arrivano anche le cc.dd. sentenze *Kadi*⁴⁸⁹, ove si censura l’omessa e immotivata comunicazione dei motivi per i quali una determinata persona viene inclusa nella *black list* dei sospettati di terrorismo dal Consiglio di sicurezza ONU, subendo di conseguenza il congelamento dei beni ai sensi del regolamento (CE) n. 881/2002⁴⁹⁰.

La Corte osserva come la procedura in esame debba realizzare una restrizione proporzionata del diritto di difesa e del diritto alla tutela giurisdizionale sanciti dall’ art.

⁴⁸⁵ Su tali tre verifiche, l’osservazione è di M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull’ordine europeo di indagine penale*, in *Riv. pen. cont.*, 4, 2015, p. 92; R. PICCIRILLO, *I profili funzionali e strutturali dell’Ordine europeo di indagine penale*, in AA.VV., *L’ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 71.

⁴⁸⁶ Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, C-293/12 e C-594/12.

⁴⁸⁷ Direttiva 2006/24/CE del 15 marzo 2006. Sulla direttiva, M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, cit., p. 306 ss.

⁴⁸⁸ Cfr. Corte EDU, 4 dicembre 2008, *S. e Marper c. Regno Unito*, punti 66 s.

⁴⁸⁹ Corte di giustizia, 18 settembre 2013, *Commissione europea e altri c. Kadi*, C-584/10 P, C-593/10 P e C-595/10 P, § 97 s. (c.d. *Kadi III*) e C. giust. UE, 3 settembre 2008, *Kadi e altro c. Consiglio dell’Unione europea e Commissione delle Comunità europee*, C-402/05 P e C-415/05 P, § 278 s. (c.d. *Kadi II*).

⁴⁹⁰ Il riferimento è al Regolamento (CE) n. 881/2002 del Consiglio, del 27 maggio 2002, che impone specifiche misure restrittive nei confronti di determinate persone ed entità associate a Osama bin Laden, alla rete Al-Qaeda e ai Talebani e abroga il regolamento (CE) n. 467/2001 che vieta l’esportazione di talune merci e servizi in Afghanistan, inasprisce il divieto dei voli e estende il congelamento dei capitali e delle altre risorse finanziarie nei confronti dei Talebani dell’Afghanistan, in GU L 139 del 29 maggio 2002. Sulle problematiche concernenti la limitazione del diritto alla protezione dei dati e del diritto alla privacy sollevate dall’applicazione del Regolamento (CE) n. 881/2002, M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, cit., p. 150 ss.

41, comma 2 e dall'art. 47 della Carta dei diritti fondamentali dell'Unione europea. Infatti, l'omessa comunicazione delle ragioni dell'inclusione nella *black list* deve esser giustificata da specifici motivi. Solo questi sono idonei a giustificare la mancata comunicazione. In assenza di questi si ravvisa una lesione dei diritti fondamentali.

Per quanto riguarda, invece, lo specifico tema della cooperazione giudiziaria, le decisioni della Corte di giustizia sono nettamente sbilanciate a favore degli obiettivi dell'Unione europea, poiché invocano spesso il primato, l'unità e l'effettività del diritto dell'Unione europea, senza giustificare adeguatamente le restrizioni dei diritti fondamentali alla luce dei principi di equivalenza e di proporzionalità⁴⁹¹.

Questo sbilanciamento è particolarmente evidente nella già citata sentenza *Melloni*, la quale ha ritenuto compatibile l'art. 4-*bis* della decisione quadro relativa al mandato di arresto europeo con il diritto di difesa e il diritto all'equo processo individuati agli art. 47 e 48, comma 2 della Carta dei diritti fondamentali dell'Unione europea.

La vicenda riguardava un ordine emanato dall'Italia relativo alla consegna da parte della Spagna di una persona condannata in contumacia per il reato di bancarotta fraudolenta. Ora, secondo l'art. 4-*bis* della decisione-quadro sul MAE, l'autorità giudiziaria di esecuzione (in questo caso la Spagna) non potrebbe rifiutare la consegna del condannato a seguito di un processo *in absentia*, quando questi abbia conferito comunque un mandato a un difensore, e il difensore lo abbia rappresentato nel corso del giudizio. Però, l'ordinamento spagnolo prevede uno *standard* di tutela più elevato secondo cui la consegna può esser disposta soltanto qualora al condannato contumace sia stata concessa un'ulteriore possibilità di impugnare la decisione⁴⁹². La Corte di giustizia ritiene che vada disapplicato lo *standard* di garanzia più elevato previsto dallo Stato spagnolo, privilegiando la realizzazione dell'obiettivo dell'Unione di una rapida, effettiva ed efficace consegna dei condannati, con conseguente sacrificio del più alto livello di protezione dei diritti fondamentali contemplato dallo Stato di esecuzione⁴⁹³.

Partendo dall'interpretazione dell'art. 4-*bis* della decisione quadro MAE, la Corte di giustizia ha motivato la sua decisione sulla base di due interessanti argomentazioni: l'art. 4-*bis* della decisione quadro MAE non solo sarebbe espressione del «consenso raggiunto dagli Stati membri nel loro insieme a proposito della portata da attribuire» ai diritti fondamentali in gioco, ma imporrebbe anche un livello di garanzie analogo a quello richiesto dalla Corte europea dei diritti dell'uomo, secondo la quale il diritto dell'accusato di partecipare al processo non è inderogabile, e ben può esser oggetto di rinuncia implicita, attraverso, ad esempio, la nomina di un difensore di fiducia⁴⁹⁴.

⁴⁹¹ Così M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, cit., p. 93.

⁴⁹² *Tribunal Constitucional* spagnolo del 5 giugno 2006, n.177/2006 e del 28 settembre 2009 n.199/2009.

⁴⁹³ Sul tema si vedano le interessanti osservazioni di S. CIVELLO CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell'Unione Europea*, cit., p. 5 s.; T. EPIDENDIO, *Il caso Melloni: il nodo irrisolto del massimo standard di tutela dei diritti fondamentali*, cit., p. 453.

⁴⁹⁴ Si guardi, *ex multis*, Corte EDU, 1° marzo 2006, *Sejdicovic c. Italia*, punti 84 ss., ove si ammette la derogabilità del diritto dell'imputato a partecipare al processo attraverso una rinuncia implicita operata con il conferimento del mandato ad un difensore di fiducia. In dottrina, *ex multis*, si legga G. DALIA, *Il processo contumacia*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), Torino, 2012, p. 485; A. BIGIARINI, *Mandato di arresto europeo e reciproco riconoscimento delle sentenze penali nei processi in absentia*, in *Dir. pen. e proc.*, 8/9, 2016, p. 999 ss.

Parte della dottrina⁴⁹⁵ ritiene corrette le conclusioni della Corte. Infatti, uno Stato che accetti di prestare la propria assistenza giudiziaria ad un altro Stato non può pretendere che quest'ultimo preveda degli *standard* di tutela dei diritti fondamentali del tutto identici a quelli previsti al proprio interno⁴⁹⁶. Ma altra parte della dottrina osserva come la Corte di giustizia non abbia giustificato la propria decisione tenendo in debita considerazione il principio di proporzionalità.

Secondo tale ultimo orientamento, la Corte non specifica per quale motivo l'attribuzione del mandato a un difensore di fiducia sia sufficiente ad assicurare il diritto di difesa e il diritto all'equo processo e sia una valida alternativa all'impugnazione della sentenza da parte del condannato *in absentia*. Sembra esserci, quindi, una violazione del principio di proporzionalità⁴⁹⁷.

Ben più evidente violazione del principio di proporzionalità è contenuta nella sentenza *Radu*, dove la Corte EDU esclude che sia legittimo rifiutare la consegna di un ricercato sulla base di un ordine contenuto in un mandato di arresto europeo emanato da uno Stato membro, fondato su una mancata previa audizione del ricercato da parte dell'autorità di emissione.

In pratica, la Corte di giustizia stabilisce che non è possibile rifiutare l'esecuzione del mandato di arresto europeo solo perché il ricercato non è stato sentito dall'autorità giudiziaria che ha emesso l'atto, poiché l'audizione preventiva del ricercato eliminerebbe l'"effetto sorpresa" dell'arresto e addirittura aumenterebbe, se non addirittura creerebbe, un pericolo di fuga del ricercato, annullando così l'obiettivo della rapida, efficace ed effettiva consegna del soggetto ricercato.

Infatti, per la Corte, gli artt. 14 e 19 della decisione quadro MAE, che prevedono l'audizione del ricercato in seguito all'arresto da parte dell'autorità giudiziaria di esecuzione, sarebbero di per sé idonei a garantire il diritto all'equo processo, il diritto di difesa e il diritto alla libertà personale disposti dall'art. 48 comma 2 e dall'art. 6 della Carta dei diritti fondamentali dell'Unione europea⁴⁹⁸.

La dottrina ha evidenziato come tale audizione non sia però sufficientemente garantista dei diritti del ricercato, sprigionando effetti del tutto parziali. Ciò è evidente se solo si consideri che l'autorità giudiziaria di esecuzione non può verificare la presenza dei requisiti che giustificano l'emissione di un mandato di arresto europeo, visto che la documentazione relativa al mandato si limita semplicemente a una "clausola di stile" con il quale si indica l'esistenza di un provvedimento di arresto emesso dall'autorità giudiziaria richiedente, evitando di indicare una motivazione circa l'esistenza di fatti che legittimano l'arresto stesso. Di conseguenza, non è possibile garantire a pieno il diritto alla libertà personale sancito dall'art. 5 CEDU⁴⁹⁹.

⁴⁹⁵ F. VIGANÒ, *Obblighi di adeguamento al diritto UE e "controlimiti": la Corte costituzionale spagnola si adegua, bon gré mal gré, alla sentenza dei giudici di Lussemburgo nel caso Melloni*, in *Dir. pen. cont.*, 9 marzo 2014.

⁴⁹⁶ Sul punto si veda anche C. AMALFITANO, *Mandato d'arresto europeo: reciproco riconoscimento vs diritti fondamentali? Note a margine delle sentenze Radu e Melloni della Corte di giustizia*, cit., p. 11 s.; G. DE AMICIS, *All'incrocio tra diritti fondamentali, mandato di arresto europeo e decisioni contumaciali: la Corte di giustizia e il "caso Melloni"*, in *Dir. pen. cont.*, 7 giugno 2013, p. 12 s.

⁴⁹⁷ Così M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Riv. pen. cont.*, 4, 2015, p. 94.

⁴⁹⁸ Così C. Giust. UE, 29 gennaio 2013, *Radu*, C-396/11, § 38 ss.

⁴⁹⁹ Cfr. M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, cit., p. 94; R. PICCIRILLO, *I profili funzionali e strutturali dell'Ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. Marafioti), cit., p. 73. Per un approfondimento sulla sentenza *Radu* e le sue lacune si rinvia a S. CIVELLO

Di recente, si è sviluppato un nuovo orientamento con la già citata sentenza *Dorobantu*, la quale impone definitivamente la centralità dei diritti fondamentali⁵⁰⁰, basati sul concetto di dignità umana. Proprio il carattere assoluto del divieto di trattamenti inumani e degradanti prescrive, al fine di decidere sulla consegna di una persona raggiunta da un mandato di arresto europeo, di non procedere ad alcun bilanciamento con il principio di reciproca fiducia, con il principio del mutuo riconoscimento e con considerazioni relative all'efficacia della cooperazione giudiziaria in materia penale, qualora un giudice constati l'esistenza di seri e comprovati motivi di ritenere che la persona oggetto del mandato di arresto europeo correrà un rischio reale di essere sottoposta a un trattamento inumano o degradante, chiudendo di fatto all'applicazione del principio di proporzionalità.

Quindi, il diritto dell'Unione europea può comprimere i diritti fondamentali e arrivare a fissare livelli di protezione inferiori a quelli stabiliti dai vari ordinamenti e dalla CEDU solo rispettando rigorosamente i parametri individuati. Come indicato dalla giurisprudenza, però, tali limitazioni non possono operare nel caso in cui in gioco vi siano diritti a carattere assoluto, come ad esempio i trattamenti inumani o degradanti⁵⁰¹.

Tuttavia, pur non lasciando margini di operatività alla proporzionalità, lo stesso art. 52 Carta UE, nell'individuare la portata e nell'indicare il metodo interpretativo dei diritti e dei principi contenuti in essa, al par. 3 con la "clausola di equivalenza" impone che laddove la Carta contenga diritti corrispondenti a quelli garantiti dalla CEDU, il significato e la portata di essi debbano essere uguali a quelli conferiti dalla Convenzione, concedendo, però, all'Unione europea una protezione più estesa di tali diritti rispetto agli standard minimi individuati dalla Convenzione stessa.

Logica conseguenza è che, per garantire il rispetto della Carta UE, è necessario una verifica compiuta dall'autorità giudiziaria di esecuzione sul pieno rispetto dei diritti fondamentali da parte dello Stato di emissione, secondo l'orientamento della Corte EDU, ed ove esistente e più garantista, secondo l'orientamento (consolidato o meno) della

CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell'Unione Europea*, in *Dir. pen. cont.*, 3 giugno 2013.

⁵⁰⁰ La dottrina ritiene che con tale sentenza la Corte abbia ulteriormente esplicitato e rafforzato la sua sensibilità per la tutela dei diritti fondamentali, ritenuti prevalenti rispetto all'effettivo funzionamento del MAE, tanto da rappresentare un punto di arrivo che difficilmente potrà essere rimesso in discussione. Sul punto, M. GIALUZ, E. GRISONICH, *Crisi dell'Unione europea e crepe nel reciproco riconoscimento: il dialogo costruttivo tra le Corti assicura il rispetto dei diritti fondamentali e l'efficacia del mandato di arresto europeo*, in *Cass. pen.*, 7-8, 2020, p. 2669. V., inoltre, M. BARGIS, *L'attuazione della direttiva (UE) 2016/1919 nei procedimenti di esecuzione del mandato di arresto europeo fra scelte positive e lacune strutturali*, in *Sistema penale*, 11, 2019, p. 85.

⁵⁰¹ Sul tema, M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, cit., p. 145; M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Diritto penale contemporaneo*, 4, 2015, p. 92; R. PICCIRILLO, *I profili funzionali e strutturali dell'ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 71. Volendo, v. anche A. GAUDIERI, *Mandato di arresto europeo: la Corte di Giustizia si pronuncia sul delicato tema della sospensione della misura detentiva ai fini della consegna*, in *slsg.unisa.it*, febbraio 2019, p. 8 ss.; disponibile al link: https://www.unisa.it/uploads/14394/audieri.febraio_2019.pdf. Secondo L. PANELLA, *Mandato di arresto europeo e protezione dei diritti umani: problemi irrisolti e "incoraggianti" sviluppi giurisprudenziali*, cit., p. 12 ss., «Il principio di proporzionalità nel diritto europeo della cooperazione penale, infatti, è un principio fondamentale che non costituisce soltanto un elemento di bilanciamento tra gli interessi della persona perseguita e l'esecuzione di una sentenza di condanna, ma [...] è anche l'elemento che permette di dare maggiore stabilità alla reciproca fiducia nella cooperazione penale europea, di cui costituisce un elemento imprescindibile».

CGUE, potendo i due indirizzi “integrarsi” – e, dunque, nel tempo interagire – al fine di individuare un equilibrio dato dal bilanciamento dei diritti e dei valori di volta in volta indicati.

Del resto, il livello di protezione della Carta UE, attraverso la “clausola di compatibilità”, non può in nessun modo calare al di sotto di tale soglia, poiché nessuna disposizione della Carta UE può essere interpretata come limitativa o lesiva dei diritti dell’uomo e delle libertà fondamentali riconosciuti in particolare dalla CEDU.

Da ciò sembra che il sistema previsto dagli art. 53 Carta UE, più che calibrato sul principio della proporzionalità in senso stretto, si basi anche sul più ampio criterio della ragionevolezza.

Invero, come rilevante dottrina fa notare, la proporzionalità non può essere semplicisticamente ridotta a mero criterio numerico, bensì si dovrebbe parlare di “ragionevolezza della proporzione”⁵⁰², nella ricerca di un punto di equilibrio nei rapporti tra autorità e libertà⁵⁰³.

Ed invero, se la proporzione fosse mero calcolo numerico, sarebbe sicuramente criterio meno indeterminato della ragionevolezza. Tuttavia, stabilire se due principi, diritti o interessi siano tra loro proporzionati significa operare una serie di valutazioni e giudizi assiologici che difficilmente comportino un risultato univoco.

Come avvenuto con le recenti sentenze della Corte di giustizia, gli interpreti hanno ritenuto di individuare un equilibrio in soluzioni non univocamente individuate secondo dogmi assoluti ed imm modificabili da applicare con un’attenzione logico-razionale, ma attraverso l’interpretazione di principi con cui conseguire un risultato ragionevolmente accettabile in virtù del *volksgeist europeo*, ossia un comune sostrato culturale, politico e sociale. Non il trionfo del relativismo, ma l’affermazione di un nuovo positivismo che, seppur lascia spazio a evidenti elasticità, è basato su criteri morali ed etici comuni al popolo europeo.

13. L’attenzione dell’Unione europea al tema della prova elettronica

Il tema delle nuove tecnologie e, più nello specifico, della prova elettronica, costituisce uno degli elementi centrali del dibattito nell’Unione europea⁵⁰⁴. Lo dimostra

⁵⁰² Così, G. SILVESTRI, *L’individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale ASPP – Salerno, 25-27 ottobre 2018 (a cura di L. KALB), cit., p. 31.

⁵⁰³ Cfr., L. KALB, *Introduzione*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale ASPP – Salerno, 25-27 ottobre 2018 (a cura di L. KALB), Milano, 2019, p. 18.

⁵⁰⁴ Sulle nuove tecnologie nel mondo del diritto, in dottrina, *ex multis*, F. ALONZI, *L’escalation dei mezzi di intrusione nella sfera privata: ripartire dalla Costituzione*, in *Rev. Bras. de Dereito Processual Penal*, 3, 2019, p. 1421 ss.; E. AMODIO, *Il processo come gioco tra letteratura e diritto vivente*, in *Riv. It. Dir. e Proc. Pen.*, 4, 2020, p. 1671 ss.; G.M. BACCARI, C. CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d’insieme*, in *Dir. pen. proc.*, 6, 2021, p. 711 ss.; F. BASILE, *Intelligenza artificiale e diritto penale. Quattro possibili percorsi di indagine*, in *Diritto penale e uomo*, 19 settembre 2019; C. CESARI, *L’impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. De Dereito Processual Penal*, 3, 2019, p. 1167 ss.; B. GALGANI, *Digitalizzazione e processo penale*, in *Questione giustizia*, 19 gennaio 2021, disponibile al link: <https://www.questionegiustizia.it/articolo/digitalizzazione-e-processo-penale>; M. GIALUZ, *Quando la giustizia penale incontra l’intelligenza artificiale: luci e ombre del risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2009; S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Berlino, 2020; ID.,

la costante attenzione che gli organi e le istituzioni le riservano, volta a sviluppare un'armonica disciplina comune, basata su principi e valori di matrice europea.

Tuttavia, il lungo e tortuoso cammino verso una disciplina completa ed esaustiva è ancora all'inizio, complici una difficoltà di approccio al tema – anche di tipo metodologico – e l'ampio ventaglio di problemi ancora rimasti irrisolti. Invero, le questioni sorte prestano il fianco a molteplici dubbi, infinite domande, poche certezze.

La consapevolezza di uno sviluppo sistematico serio e concreto del tema nasce dal ruolo ormai preponderante che assumono le prove elettroniche all'interno di un processo penale. Gli strumenti tecnologici sono i nuovi «occhi ed orecchie della giustizia»⁵⁰⁵. Consentono un accesso più immediato e sovente più oggettivo alla materialità del fatto-reato. La loro fragilità, d'altro canto, comporta la necessaria individuazione di procedimenti e tecniche che ne garantiscano la genuinità, l'attendibilità e la conservazione.

Proprio tali caratteristiche nascondono insidie ed insicurezze, le quali lasciano affiorare nell'interprete un profondo dilemma relativo al ruolo – *rectius*, alla funzione – che possa avere nei procedimenti penali una prova digitale, informatica, elettronica.

La centralità che ha assunto, sta assumendo ed assumerà la prova digitale comporta una profonda riflessione sulle tradizionali *regolae iuris* che informano l'acquisizione e l'utilizzo del contributo conoscitivo proveniente da esse. Nondimeno, comporta anche profonde angosce in coloro i quali debbono, all'evidenza, comprenderne non solo la portata, ma anche i limiti che essa mostra in un giusto processo, pienamente rispettoso dello Stato di diritto nonché dei diritti fondamentali universalmente, europeisticamente e costituzionalmente riconosciuti.

Già nel 2010 la Commissione europea poneva attenzione al tema delle nuove tecnologie, formulando obiettivi strategici⁵⁰⁶. Essa ravvisava correttamente nella criminalità informatica una minaccia crescente, che si manifesta sotto varie forme, tra cui quella della criminalità organizzata e del terrorismo.

L'interesse della Commissione nasceva dalla consapevolezza che l'Europa – come del resto larga parte del globo terracqueo – sia divenuto un bersaglio chiave per la sua infrastruttura Internet avanzata, l'alto numero di utenti e il fatto che i circuiti economici e i sistemi di pagamento sono supportati dal web. Non va dimenticato, poi, che tratta di esseri umani, traffico di stupefacenti e armi da fuoco, riciclaggio di denaro, spedizione e scarico illegale di rifiuti, nonché reati apparentemente meno gravi quali i furti con scasso e i furti di auto, la vendita di merci contraffatte e pericolose e le azioni messe a segno dalle gang itineranti sono spesso manifestazioni di reti criminali mondiali che ravvisano

Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per una urgente discussione tra scienze penali e informatiche, in *La Legislazione penale*, 18 dicembre 2018; T. RAFARACI, *Verso una law of evidence dei dati*, in *Dir. Pen. proc.*, 7, 2021, p. 853 ss. Più nello specifico, sul tema delle attività di carattere investigativo, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 121 ss.

⁵⁰⁵ In questi termini, riferendosi però ai testimoni, si esprimeva G. BENTHAM, *Teoria delle prove giudiziarie*, Bruxelles, 1842.

⁵⁰⁶ Cfr., Comunicazione della Commissione al Parlamento europeo e al Consiglio, *La strategia di sicurezza interna all'UE in azione: cinque tappe verso un'Europa più sicura*, COM(2010) 673. La comunicazione individua le sfide più urgenti in materia di sicurezza cui l'UE deve far fronte, proponendo cinque obiettivi strategici modulati sulla collaborazione tra Stati membri e istituzioni dell'UE al fine di garantire una maggior efficacia nel combattere e prevenire le forme gravi di criminalità organizzata, il terrorismo e la criminalità informatica, nonché nel rafforzare la gestione delle frontiere esterne e costruire la resilienza alle calamità naturali e provocate dall'uomo.

nel ciberspazio il loro *humus* ideale dove proliferare, e nelle nuove tecnologie gli strumenti adeguati per consumare reati, garantendosi spesso l'impunità.

Per la Commissione è, dunque, necessario che i cittadini, le imprese, le infrastrutture pubbliche e private godano di una maggiore protezione dalle forme di criminalità che sfruttano le tecnologie moderne.

La sicurezza informatica diventa fattore essenziale per il buon andamento della società dell'informazione al fine di evitare il “*cyber far west*”, nonché di combattere ed arginare lo sviluppo e l'applicazione rapida delle nuove tecnologie dell'informazione da parte delle nuove forme di attività criminale, le quali provocano danni ingenti ai Paesi dell'Ue ed all'Unione europea stessa⁵⁰⁷.

Tutto ciò va considerato alla luce di un sistema di interessi e valori che l'Unione già garantisce *offline*. All'evidenza, i principi e i valori alla base dell'organizzazione *sui generis* devono per forza di cose essere estesi anche al variegato mondo virtuale che si è soliti definire con il termine “ciberspazio” al fine di assicurare che esso rimanga aperto e libero. Ciò diventa tanto più importante se solo si riflette sull'imponente espansione del *web* negli ultimi decenni.

Esso ha avuto un impatto impressionante su tutti gli strati della società e nondimeno ha inciso radicalmente sulla vita quotidiana. Ne deriva che i diritti fondamentali, le interazioni sociali e le economie tendono a dipendere in maniera preponderante dal funzionamento impeccabile delle nuove tecnologie dell'informazione e della comunicazione.

Ed allora, se un ciberspazio aperto e libero ha promosso l'inclusione politica e sociale in tutto il mondo, ha abbattuto barriere tra Paesi, comunità e cittadini rendendo possibile l'interazione e lo scambio di informazioni e di idee in tutto il pianeta, ha anche creato un importante *forum* di libertà di espressione ed esercizio dei diritti fondamentali di indubbio interesse per l'Unione europea, la quale ne ha ravvisato un solido fondamento per la società democratica e giusta⁵⁰⁸.

Tuttavia, uno spazio aperto e libero – quale si propone di essere il ciberspazio – presuppone la sicurezza. Per l'Unione europea è, dunque, fondamentale proteggerlo da incidenti, attività dolose ed abusi⁵⁰⁹, anche mediante strumenti che garantiscano il rispetto

⁵⁰⁷ La sicurezza delle reti informatiche è stata riconosciuta con la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un'agenda digitale europea*, COM(2010) 245, nella quale sono trattate le questioni legate alla criminalità informatica, alla sicurezza informatica, all'uso sicuro di Internet e alla privacy quali presupposti per instaurare un clima di fiducia e di sicurezza per gli utenti della rete.

⁵⁰⁸ In tal senso, Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e la Comitato delle Regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1 final. Con tale comunicazione, si propone una strategia per la cibersicurezza, delineando la visione dell'UE in questo campo, chiarendo i ruoli e le responsabilità, definendo gli interventi necessari per una protezione effettiva e forte e per la promozione dei diritti dei cittadini, nell'intento di fare dell'ambiente *online* dell'Unione l'ambiente in linea più sicuro al mondo.

⁵⁰⁹ Con le conclusioni sul *Piano d'azione dell'UE per i diritti umani e per la democrazia 2020-2024* del 18 novembre 2020, 12848/20, il Consiglio ha osservato che «New technologies can contribute significantly to the protection and promotion of human rights and democracy, including by making public participation easier and more effective, increasing access to public services, facilitating the documentation of violations and abuses, and supporting online activism. However, these technologies can also have a negative impact, such as spreading disinformation and hate speech, enabling new forms of violence, violations and abuses of the right to privacy, facilitating access to specific illegal content including child exploitation, widespread surveillance limiting freedom of expression and reducing civil society space, reinforcing discrimination and structural inequalities. This possible negative impact must be prevented and countered». Inoltre, ritiene che è necessario «Protect the individual's right to privacy and data protection,

e la protezione dei diritti fondamentali in internet⁵¹⁰. In questo scenario si inserisce non solo una strategia volta all'individuazione di strumenti condivisi per la formazione delle prove elettroniche, ma anche lo sviluppo di tecnologie investigative che consentano di impedire ai cybercriminali di consumare reati cibernetici con metodi sempre più avanzati. Ciò ha spinto gli Stati membri e l'Unione europea a considerare il ciberspazio come una questione internazionale sempre più importante.

Del resto, una maggiore connettività da un lato favorisce servizi digitali, dall'altro può far sì che i cittadini, le imprese e le amministrazioni si trovino esposte a minacce e reati informatici sempre più numerosi e sofisticati. Per questo il Consiglio ha recentemente sottolineato l'importanza di salvaguardare l'integrità, la sicurezza e la resilienza delle infrastrutture critiche, delle reti, dei servizi e dei terminali di comunicazione elettronica⁵¹¹.

Difatti, più si sviluppa il mondo digitale, più aumentano le occasioni da sfruttare: le tecniche utilizzate dai cybercriminali sono sempre più all'avanguardia. Per questo è necessario sviluppare strumenti operativi giusti e capacità adeguate a fronteggiarli. Il crimine ormai non conosce confini: l'estensione planetaria di internet implica che l'attività di contrasto deve essere coordinata e sostenuta dalla collaborazione transnazionale, in funzione di una solerte risposta alla crescente minaccia che si appalesa davanti agli occhi del mondo intero.

Pertanto, già da tempo, l'Unione europea e gli Stati membri hanno compreso la necessità di dotarsi di una legislazione solida ed efficace per affrontare il cybercrimine, affiancata dal forte sviluppo di tecniche di contrasto informatico con strumenti operativi di ultima generazione, dall'individuazione di buone pratiche e delle migliori tecniche disponibili per lottare contro la cybercriminalità⁵¹², dalla collaborazione reciproca tra Stati nonché con le agenzie e gli organismi dell'Unione europea⁵¹³ per armonizzare gli approcci strategici con le migliori pratiche sul fronte operativo⁵¹⁴.

Già nel 2015 con l'Agenda europea sulla sicurezza, la Commissione si è impegnata a riesaminare gli ostacoli alle indagini penali, ponendosi una serie di obiettivi. In particolare, «la criminalità informatica esige che le autorità giudiziarie competenti ripensino al modo in cui cooperano nell'ambito delle loro giurisdizioni e della legge applicabile per garantire un accesso transfrontaliero più rapido alle prove e alle informazioni, tenendo conto degli sviluppi tecnologici attuali e futuri, quali il *cloud computing* e l'«internet delle cose». La raccolta delle prove elettroniche in tempo reale da

including in the context of digital space and with respect to disproportionate government access and control» nonché «Promote an open, free and secure internet, including by monitoring internet shutdowns, online censorship and digital practices such as those leading to mass arbitrary surveillance while supporting efforts to protect freedom of expression, media freedom and pluralism in the online environment».

⁵¹⁰ Sul rispetto dei diritti fondamentali in internet, A. IERMANO, *Verso un nuovo diritto "fondamentale" in ambito UE: il diritto alla disconnessione digitale*, in *Eurojus*, 2, 2021, p. 150 ss.; R. PALLADINO, *Sul diritto all'oblio e la tutela dei diritti fondamentali in internet: ambito di applicazione territoriale e bilanciamento a margine della sentenza Google LLC della Corte di giustizia dell'UE*, in *I diritti dell'uomo*, 3, 2019, p. 543 ss.

⁵¹¹ Cfr., Conclusioni del Consiglio *Plasmare il futuro digitale dell'Europa* del 9 giugno 2020, (2020/C 202 I/01).

⁵¹² Ad esempio, lo sviluppo e l'uso di strumenti di polizia scientifica e l'analisi delle minacce.

⁵¹³ Il riferimento è al Centro europeo per la lotta alla criminalità informatica (EC3), all'Europol, ad Eurojust e ad EPPO.

⁵¹⁴ Cfr., Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e la Comitato delle Regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1 final.

altre giurisdizioni su questioni quali i proprietari di indirizzi IP o altre prove elettroniche, e la loro ammissibilità dinanzi al giudice sono questioni di importanza fondamentale. È inoltre necessario che il personale delle autorità di contrasto sia altamente qualificato, in grado di tenere il passo con l'aumento considerevole della portata, della sofisticazione e dei tipi di reati informatici»⁵¹⁵.

Il Consiglio ha riconosciuto che combattere l'uso improprio di Internet a fini terroristici è fondamentale nella lotta contro la propaganda terroristica ed estremista violenta⁵¹⁶. È necessario però salvaguardare, allo stesso tempo, i diritti umani. Per cui non solo ha ribadito la necessità di una normativa europea che impedisca la diffusione di contenuti terroristici illegali online, ma ha anche considerato che lo sviluppo tecnologico può essere utilizzato per scopi illeciti. Di talché, ha auspicato una massimizzazione dei benefici provenienti dalle nuove tecnologie a favore dei servizi di sicurezza e per contrastare l'uso improprio delle nuove tecnologie da parte dei terroristi⁵¹⁷.

Per avviare un processo di accelerazione della transizione digitale in Europa, il Consiglio europeo aveva invitato la Commissione a presentare entro marzo 2021 una “bussola per il digitale” (*Digital Compass*) globale che definisca le ambizioni digitali concrete dell'UE all'orizzonte 2030.

Ed infatti, nel marzo 2021, la Commissione ha pubblicato la “*Bussola per il digitale 2030: il modello europeo per il decennio digitale*”⁵¹⁸, in cui ha indicato la necessità di istituire un sistema di monitoraggio delle capacità e abilità digitali strategiche europee e delineare i mezzi e le tappe principali per realizzare le ambizioni prospettate⁵¹⁹.

Con questo documento, la Commissione ha manifestato esplicitamente l'ambizione di perseguire politiche per il digitale che conferiscano ai cittadini e alle imprese l'autonomia e la responsabilità necessarie per conseguire un futuro digitale antropocentrico, sostenibile e più prospero.

In tale contesto, all'interno di un nuovo pacchetto sulla sicurezza che prevede misure legislative dirette a ridurre il margine di manovra dei terroristi e degli altri criminali⁵²⁰, è maturato il progetto di una proposta di regolamento relativo agli ordini europei di

⁵¹⁵ Cfr., Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 28 aprile 2015, *Agenda europea sulla sicurezza*, COM(2015) 185 final.

⁵¹⁶ In particolare, la Commissione promuove e favorisce la cooperazione con piattaforme internet per individuare e rimuovere contenuti illeciti online terroristici o di altra natura. V., Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio, *Quattordicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza* del 17 aprile 2018, COM(2018) 211 final.

⁵¹⁷ Cfr., Conclusioni del Consiglio sull'azione esterna dell'UE per la prevenzione e la lotta contro il terrorismo e l'estremismo violento del 15 giugno 2020, 8868/20.

⁵¹⁸ Cfr., Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni “*Bussola per il digitale 2030: il modello europeo per il decennio digitale*” del 9 marzo 2021, COM(2021) 118 final.

⁵¹⁹ Cfr., Conclusioni del Consiglio europeo del 1° e 2 ottobre 2020, EUCO 13/20.

⁵²⁰ Il pacchetto comprende misure legislative dirette a migliorare l'accesso transfrontaliero alle prove elettroniche e alle informazioni finanziarie ai fini delle indagini e delle azioni penali; misure operative per impedire l'accesso di terroristi ed altri criminali alle armi da fuoco importate e ai precursori di esplosivi che possono essere impropriamente utilizzati per la fabbricazione di esplosivi artigianali; una proposta legislativa volta a migliorare la sicurezza delle carte d'identità e dei titoli di soggiorno nazionali, il cui obiettivo è rendere più difficile per i terroristi e altri criminali abusare di tali documenti o falsificarli per entrare o spostarsi in UE. V., Comunicazione della Commissione e del Parlamento europeo, al Consiglio europeo e al Consiglio “*Quattordicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza*”, COM(2018) 211 final.

produzione e di conservazione di prove elettroniche nei procedimenti penali⁵²¹ e una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali⁵²².

14. (Segue). Verso nuovi strumenti per la formazione della prova elettronica transnazionale

Per la circolazione transnazionale delle prove – incluse le elettroniche – si fa riferimento ad un quadro normativo fortemente variegato. Si tratta di un “dedalo normativo” caratterizzato da una elefantica produzione che ne rende estremamente difficile una lettura sistematica.

Accanto ad una cospicua serie di convenzioni bilaterali, vi sono numerose convenzioni multilaterali che prevedono la possibilità di impiegare strumenti della cooperazione giudiziaria per formare una prova a vocazione transnazionale. È comunque lasciata alla discrezionalità dei singoli Stati l'applicazione di eventuali disposizioni più favorevoli contenute nei singoli accordi bilaterali tra Stati.

Tra le convenzioni multilaterali a cui si fa riferimento vi sono la Convenzione europea di assistenza giudiziaria in materia penale del 1959 ed i suoi due relativi Protocolli addizionali⁵²³, la Convenzione di applicazione degli Accordi Schengen del 1990⁵²⁴ e la Convenzione sulla mutua assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea del 2000 (M.A.P.)⁵²⁵, detta anche Convenzione di Bruxelles.

Inoltre, con la direttiva 2014/41/UE l'Unione europea ha istituito lo strumento dell'ordine europeo di indagine (OEI)⁵²⁶, il quale prevede una comunicazione diretta tra autorità giudiziarie; termini brevi; l'impiego di moduli *standard*; una limitata possibilità di rifiutare l'esecuzione delle richieste.

Tuttavia, le richieste richiedono ancora un tempo di elaborazione poco ragionevole. Soprattutto per le prove elettroniche – di natura volatile e di facile trasmissione, modificazione e cancellazione – le procedure di assistenza giudiziaria reciproca sono considerate inadeguate.

⁵²¹ COM(2018) 225 final del 17 aprile 2018.

⁵²² COM(2018) 226 final del 17 aprile 2018.

⁵²³ Ratificata dall'Italia con l. 23 febbraio 1961, n. 215 ed entrata in vigore il 12 giugno 1962. Il primo Protocollo addizionale è stato fatto a Strasburgo il 17 marzo 1978 (ETS n.099), in vigore dal 12 aprile 1982 e ratificato dall'Italia con l. 24 luglio 1985, n. 436, mentre il secondo Protocollo addizionale dell'8 novembre 2011 e firmato dall'Italia il 23 gennaio 2013, è stato ratificato con l. 24 luglio 2019, n. 88.

⁵²⁴ Si tratta della Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, in GUUE L 236 del 22 settembre 2000 a cui l'Italia ha aderito con l'Accordo di adesione della Repubblica italiana alla Convenzione di applicazione dell'Accordo di Schengen del 14 giugno 1985 tra i governi degli Stati dell'Unione economica Benelux, della Repubblica federale di Germania e della Repubblica francese relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmato a Schengen il 19 giugno 1990, in GUUE L 239 del 22 settembre 2000.

⁵²⁵ In GUCE C 197 del 12 luglio 2000, attuata in Italia con D. Lgs. 5 aprile 2017 n. 52, in GU 27 aprile 2017, n. 97. Per un approfondimento, si legga S. MONICI, *Emanate le norme di attuazione della convenzione di assistenza giudiziaria in materia penale del 29 maggio 2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo di indagine?*, in *Eurojus*, 3 maggio 2017.

⁵²⁶ In GUUE L 130 del 1° maggio 2014, attuata in Italia con D. Lgs. 21 giugno 2017, n. 108, in GU 13 luglio 2017, n. 162.

Il quadro giuridico si completa con: il Regolamento (UE) 2018/1727 del Parlamento europeo e del Consiglio che istituisce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust) e che sostituisce e abroga la decisione 2002/187/GAI del Consiglio⁵²⁷; il Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol)⁵²⁸; il Regolamento (UE) 2017/1939 relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO»)⁵²⁹; la decisione quadro 2002/465/GAI del Consiglio relativa alle squadre investigative comuni⁵³⁰; gli accordi bilaterali tra l'Unione europea e Paesi terzi, quali gli accordi sull'assistenza giudiziaria con gli USA⁵³¹ e con il Giappone.

Per quanto riguarda l'ordinamento italiano, va menzionata la disciplina sussidiaria e residuale prevista per le rogatorie internazionali agli art. 723 ss. c.p.p. e dalla particolare disposizione prevista dall'art. 234-*bis* c.p.p. in tema di acquisizione di documenti e dati informatici.

Conclude l'elenco delle fonti, seppur parzialmente, la Convenzione nata in seno al Consiglio d'Europa sulla criminalità informatica, contenente una serie di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati ed il cui obiettivo principale, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la cibercriminalità, in special modo adottando legislazioni appropriate e promuovendo la cooperazione internazionale.

L'insieme estremamente variegato delle fonti relative alla disciplina sull'acquisizione transfrontaliera delle prove ha creato forti imbarazzi e profonde incertezze negli interpreti, i quali, nel dover mettere ordine al fine di individuare la normativa corretta da applicare al caso concreto, spesso si trovano a dover interpretare un quadro normativo estremamente complesso.

È stata di fatto creata una forte stratificazione normativa che appare a tratti confusionaria: vi sono convenzioni che regolano i rapporti con i Paesi extraeuropei e quelle che regolano i rapporti con Paesi europei. Tra i Paesi europei vi è da distinguere i rapporti con i Paesi che fanno parte del Consiglio d'Europa e i Paesi che fanno parte anche dell'Unione europea; tra questi, debbono distinguersi quelli dell'Area Schengen, ai quali è affiancata un'ulteriore disciplina.

Gli strumenti sinora citati sono stati elaborati al fine di trattare i casi in cui le prove o il prestatore di servizi si trovino all'estero. Purtroppo, nonostante le riforme periodicamente in atto, i meccanismi di cooperazione subiscono una pressione crescente a causa della maggiore necessità di un accesso tempestivo alle prove elettroniche a livello transfrontaliero.

La frammentazione che ne è derivata ha generato incertezza giuridica e obblighi contrastanti, con effetti negativi sulla protezione dei diritti fondamentali e delle garanzie procedurali delle persone interessate.

⁵²⁷ In GUUE L 295 del 21 novembre 2018.

⁵²⁸ In GUUE L 135 del 24 maggio 2016.

⁵²⁹ In GUUE L 283 del 31 ottobre 2017.

⁵³⁰ In GUCE L 162 del 20 giugno 2002.

⁵³¹ Si tratta della decisione 2009/820/PESC del Consiglio, del 23 ottobre 2009, relativa alla conclusione, a nome dell'Unione europea, dell'accordo sull'extradizione tra l'Unione europea e gli Stati Uniti d'America e dell'accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, in GUUE L 291 del 7 novembre 2009.

Ad oggi, questi strumenti non consentono di arginare a pieno le difficoltà nell'accesso transfrontaliero alle prove elettroniche, con conseguente lesione delle indagini e dei procedimenti penali nell'Unione europea. Essi si caratterizzano per la lentezza, poiché concepiti per le prove fisiche, prevedendo spesso tempi di trasmissione dei risultati non adatti alla velocità con cui si modificano e si muovono gli elementi informatici nella rete⁵³².

Due sono le dimensioni da considerare nell'attuale mondo governato dalle nuove tecnologie: lo spazio ed il tempo. Il tempo è essenziale per permettere alle autorità di ottenere dati indispensabili; lo spazio rileva nelle "situazioni transfrontaliere" in cui spesso si trovano ad operare le autorità giudiziarie, in special modo quando risultano rilevanti elementi elettronici, digitali, informatici, poiché di frequente vi è il coinvolgimento di un prestatore di servizi straniero e le informazioni sono conservate elettronicamente in un altro Stato membro.

Risulta particolarmente vulnerata l'efficienza nella cooperazione giudiziaria tra autorità pubbliche, nella cooperazione diretta tra autorità pubbliche e prestatori di servizi (i cc.dd. *Internet service provider*) e nell'accesso diretto delle autorità pubbliche alle prove elettroniche. Conseguenza scontata è l'arresto delle indagini⁵³³, con evidente riflesso sull'impunità dei reati e l'abbattimento delle tutele nei confronti dei soggetti passivi coinvolti, che contribuiscono ad una percezione di insicurezza nel *cyberspace*⁵³⁴.

La sicurezza nel ciberspazio, che passa anche attraverso un efficiente sistema repressivo delle condotte riprovevoli penalmente perseguibili, diventa di primaria importanza, tanto più le reti ed i sistemi informativi nonché le reti e i servizi di comunicazione elettronica svolgono un ruolo essenziale nella società ed assurgono a pilastri della crescita economica. Esse assumono un ruolo fondamentale nelle attività quotidiane della società, contribuendo al buon funzionamento delle economie dei singoli Stati in settori essenziali quali la sanità, l'energia, la finanza, i trasporti e, in particolare, il mercato interno⁵³⁵.

Un innalzamento del livello di sicurezza, che passa anche attraverso strumenti moderni per la formazione della prova elettronica transfrontaliera, assume anche le forme di una evidente reazione alle minacce terroristiche, poiché renderebbe più difficile la progettazione e l'esecuzione delle loro azioni efferate.

Le prove informatiche hanno assunto una loro centralità ed autonoma dignità data anche dalla loro spiccata natura tendenzialmente transnazionale. La loro importanza nella

⁵³² In tal senso, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. De Direito Processual Penal*, 3, 2019, p. 1280.

⁵³³ È stato accertato che oltre la metà delle indagini penali comprende una richiesta di accesso transfrontaliero a prove elettroniche quali testi, e-mail, o applicazioni per lo scambio di messaggi. In tal senso, Parere del Comitato economico e sociale europeo sulla «Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale» e sulla «Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali», (2018/C 367/17), in GUUE, C367 del 10 ottobre 2018.

⁵³⁴ L'incremento della digitalizzazione e della connettività comporta un aumento del rischio connesso alla cibersicurezza, rendendo la società più vulnerabile alle minacce informatiche e aggravando i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori.

⁵³⁵ Cfr., *considerando* 1, regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e la certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), in GUUE, L 151 del 7 giugno 2019.

vasta maggioranza delle indagini penali è data dalla circostanza per cui sempre più spesso le autorità giudiziarie inoltrano richieste in un'altra giurisdizione per ottenere le prove necessarie da prestatori di servizi.

Sempre più spesso le autorità giudiziarie instaurano forme di cooperazione direttamente con i *provider*, fondandole sulla *voluntary disclosure*. Questa tecnica consente alle società private di decidere di volta in volta se collaborare ed in quali limiti⁵³⁶.

Di cruciale rilevanza per le indagini e per un corretto esercizio dell'azione penale – soprattutto in caso di terrorismo o criminalità informatica – è rendere più facile e più veloce l'acquisizione di tali tipi di prove transfrontaliere, in coerenza con i principi di un internet libero, aperto e sicuro senza la compromissione di diritti umani e delle libertà fondamentali⁵³⁷. Già con la direttiva 2017/541/UE, al *considerando* 7, si proponeva l'adozione di strumenti di collaborazione con i Paesi terzi per la raccolta e la formazione della prova elettronica finalizzata ad ottenere una risposta globale più efficace alla lotta al terrorismo mediante un rafforzamento della cooperazione da parte dell'Unione europea e dei suoi Stati membri con il resto del mondo⁵³⁸.

A questo scopo, l'Unione europea ha allo studio due proposte legislative volte a migliorare l'acquisizione transfrontaliera di prove elettroniche per i procedimenti penali: una proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche nei procedimenti penali e una proposta di direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali.

I due atti legislativi forniranno alle autorità di contrasto ed alle autorità giudiziarie competenti nuovi strumenti per acquisire prove elettroniche nel rispetto dei diritti e delle libertà fondamentali dei cittadini, in modo tale da rispondere con un quadro giuridico all'avanguardia e non frammentato alle sfide messe in rilievo dal Parlamento europeo e dal Consiglio⁵³⁹.

Invero, il Parlamento aveva invitato la Commissione ad avviare un *iter* legislativo che andasse in tale direzione, con la previsione di «norme armonizzate per determinare se un prestatore di servizi possa considerarsi nazionale o estero» e volte ad «imporre ai prestatori di servizi l'obbligo di rispondere a richieste provenienti da altri Stati membri basate su regolare procedura legale e in linea con l'ordine europeo di indagine (OEI),

⁵³⁶ Sul punto, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1282.

⁵³⁷ V., Conclusioni del Consiglio sull'azione esterna dell'UE per la prevenzione e la lotta contro il terrorismo e l'estremismo violento del 15 giugno 2020, 8868/20.

⁵³⁸ La direttiva 2017/541/UE del Parlamento europeo e del Consiglio del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, in GUUE L 88 del 31 marzo 2017 è stata recepita con Legge di delegazione europea 2016/2017, l. 25 ottobre 2017, n. 163. Sulla direttiva, S. CENTONZE, L. GIOVEDÌ, *La direttiva antiterrorismo 2017/541 del 15 marzo 2017*, in *Il Penalista*, 31 maggio 2017; S. DE LUCA, *La direttiva 2017/541/UE e il difficile bilanciamento tra esigenze di pubblica sicurezza e rispetto dei diritti umani*, in *Eurojus*, 3 luglio 2017; G. DUCOLI, *La lotta dell'Unione europea al terrorismo. Un primo sguardo alla direttiva UE/2017/541*, in *Leg. Pen.*, 27 luglio 2017; S. SANTINI, *L'Unione europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541*, in *dir. pen. cont.*, 7-8, 2017, p. 13 ss.

⁵³⁹ Con tali proposte la Commissione risponde agli inviti rivolti dal Parlamento europeo e dal Consiglio affinché presentasse misure legislative volte ad agevolare l'acquisizione delle prove elettroniche al di là delle frontiere. Cfr., Conclusioni del Consiglio sul miglioramento della giustizia penale nel ciberspazio (ST 9579/16) e risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica, 2017/2068 (INI).

tenendo conto del principio di proporzionalità per evitare effetti negativi sull'esercizio della libertà di stabilimento e la libera prestazione di servizi e garantire adeguate garanzie, al fine di garantire la certezza del diritto e migliorare la capacità dei prestatori di servizi e degli intermediari di rispondere alle richieste dei servizi di contrasto»⁵⁴⁰.

Con la proposta di Regolamento adottata dalla Commissione che mira a creare gli ordini di “produzione” e di “conservazione” si affronta il problema specifico della natura volatile delle prove e della loro dimensione internazionale. Il tentativo è quello di adattare i meccanismi di cooperazione all'era digitale, prevedendo anche una singolare applicazione del principio del mutuo riconoscimento mediante lo sviluppo di un moderno strumento in dotazione alle autorità giudiziarie e di contrasto, al passo con le più avanzate modalità di comunicazione dei criminali ed in grado di combattere le forme moderne di criminalità, nel pieno rispetto dei diritti, delle libertà e dei principi sanciti nella Carta dei diritti fondamentali dell'Unione europea, nonché dei diritti fondamentali garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dei principi risultanti dalle tradizioni costituzionali comuni agli Stati membri⁵⁴¹.

Obiettivo della proposta è rendere più rapido e facile il processo di formazione della prova elettronica transnazionale al fine di ottenere prove elettroniche conservate e/o detenute da prestatori di servizi stabiliti in un'altra giurisdizione. In tal modo si garantisce: una riduzione dei tempi; un sicuro accesso transfrontaliero alle prove elettroniche nei casi in cui attualmente manca; la certezza giuridica, la protezione dei diritti fondamentali, la trasparenza e la responsabilità.

Lo strumento – che si affiancherà agli attuali strumenti di cooperazione giudiziaria pertinenti e utilizzabili quando ritenuti appropriati – è volto a migliorare la certezza del diritto per le autorità, i prestatori di servizi e le persone interessate nonché a mantenere uno *standard* elevato per le richieste delle autorità di contrasto⁵⁴². Inoltre, neutralizza anche il pericolo del *forum shopping*, che consentirebbe alle autorità di uno Stato di prescegliere lo Stato dotato del sistema di maggiori capacità repressive, e quindi maggiormente disposto a trasmettere le prove⁵⁴³.

I nuovi strumenti si basano su una particolare forma di mutuo riconoscimento⁵⁴⁴, che figura all'art. 82, par.1, TFUE, perché permetteranno alle autorità competenti di uno Stato membro di ingiungere direttamente ai prestatori di servizi – come ad esempio i prestatori di servizi di comunicazione elettronica e specifici prestatori di servizi della società dell'informazione – stabiliti o rappresentati in un altro Paese dell'UE⁵⁴⁵, senza richiedere

⁵⁴⁰ V., Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica, P8_TA(2017)0366.

⁵⁴¹ Tra tali diritti e principi figurano il diritto alla libertà ed alla sicurezza, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà d'impresa, il diritto di proprietà, il diritto a un ricorso effettivo e a un equo processo, il diritto a un giudice imparziale, la presunzione di innocenza e il diritto alla/della difesa, i principi di legalità e proporzionalità, il diritto di non essere giudicato o punito due volte per lo stesso reato.

⁵⁴² In tal senso, L. BUONO, *The genesis of the European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, in *ERA Forum*, 3, 2019, p. 307 ss.

⁵⁴³ Cfr., M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1281.

⁵⁴⁴ Sul punto, che verrà successivamente approfondito, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., pp. 1277 ss.

⁵⁴⁵ Si fa riferimento ai prestatori di servizi che offrono servizi in uno o più Stati membri, a prescindere dal luogo in cui sono situate la loro sede principale e le loro infrastrutture e in cui vengono conservate le informazioni.

l'intervento dell'autorità dello Stato in cui questi siano stabiliti o rappresentati, di conservare o produrre informazioni elettroniche esistenti ai fini dell'indagine o del perseguimento dei reati, nel rispetto del principio di proporzionalità e necessità del caso specifico.

L'esigenza di rivedere per tali strumenti i criteri su cui si fonda il principio del mutuo riconoscimento, prevedendo una cooperazione tra pubblico e privato e non tra organi statuali, nasce dalla necessità di una maggior efficacia ed efficienza nella lotta a quelle manifestazioni di criminalità che utilizzano elementi informatici per le loro condotte penalmente rilevanti, al fine di ottenere un globale miglioramento della sicurezza e una sensibile riduzione della percezione di impunità per i reati commessi su dispositivi connessi in rete o loro tramite⁵⁴⁶. L'autorità giudiziaria dello Stato membro in cui il prestatore di servizi o il suo legale rappresentante è ubicato interverrà soltanto al fine di riconoscere ed eseguire l'ordine nel caso in cui il fornitore di servizi non vi si conformi.

La transnazionalità della prova elettronica, spesso collocata nei *cloud* e detenuta dai *service provider* ha contribuito al ripensamento dello schema previsto dal mutuo riconoscimento, affinché si eviti che le autorità di contrasto utilizzino mezzi propri – come, ad esempio, il *trojan* – con il rischio di danneggiare o contraffare quanto acquisito, pregiudicandone la spendibilità in giudizio⁵⁴⁷.

Per garantire la piena applicazione del Regolamento sarà necessario, con la direttiva sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali⁵⁴⁸, imporre ai prestatori di servizi di designare almeno un rappresentante legale nell'Unione europea.

Lo studio degli strumenti basati sul principio del mutuo riconoscimento per la formazione della prova elettronica caratterizzata da transnazionalità comporta l'analisi dell'attuale assetto normativo e giurisprudenziale (non solo nazionale, ma anche sovranazionale ed internazionale) previsto per essa, al fine di verificare se le discipline convergono verso una seria e concreta armonizzazione che consenta un'applicazione ordinata e sistematica delle norme previste per gli ordini europei di produzione e di conservazione.

Sembra esista una forte diversità tra legislazioni nazionali che attualmente disciplinano la prova elettronica, in particolare per quanto riguarda le garanzie e i poteri previsti. È, dunque, di fondamentale importanza sondare e scovare, nei meandri dei nuovi strumenti, eventuali vuoti normativi, questioni giuridiche discusse, incongruenze, dubbi, incertezze ma anche convergenze e potenzialità di un sistema unico nel suo genere.

Tracciato così il quadro generale, è d'uopo ricostruire dapprima la disciplina basata sul principio della mutua assistenza, così come previsto dalla Convenzione europea sulla criminalità informatica e dal relativo Secondo protocollo ad essa, nonché dal Cloud Act

⁵⁴⁶ Così, E. COLOMBO, *Ordini europei di produzione e di conservazione delle prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, in *Cass. pen.*, 7, 2019, p. 2722 ss.; V. MITSILEGAS, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, 3, 2018, p. 263 ss.

⁵⁴⁷ In tal senso, L. BARTOLI, *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *Big data and Public Law: new challenges beyond data protection*, cit., p. 102; M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1279.

⁵⁴⁸ Si fa riferimento alla proposta di direttiva del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali, COM(2018) 226 final.

statunitense, per poi illustrare le regole sviluppate dall'Unione europea per l'acquisizione delle prove elettroniche transnazionali contenute della direttiva 2014/41/UE sull'ordine europeo di indagine ed allo studio per la creazione dei due strumenti specificamente dedicati a tale attività – gli ordini europei di conservazione e di produzione – basati sul principio del mutuo riconoscimento.

Ciò consentirà di comprendere se è possibile un ravvicinamento normativo e se si sta andando in tale direzione. Inoltre, si verificherà in che modo sia stato operato un bilanciamento tra valori contrapposti, nel rispetto dei diritti fondamentali e come stanno evolvendo gli strumenti della cooperazione giudiziaria in materia penale per la formazione delle prove elettroniche transnazionali, ormai incentrati sul rapporto diretto tra autorità pubbliche e società private, al fine di dare risposta alle istanze di celerità e di garanzia, proprie del contesto digitale in cui si sviluppano.

CAPITOLO III

LA CONVENZIONE EUROPEA SULLA CRIMINALITÀ INFORMATICA E LA COOPERAZIONE CON GLI USA

Sommario: 1. La Convenzione del Consiglio d'Europa sulla criminalità informatica: un quadro generale. – 2. La mutua assistenza per la formazione dell'*e-evidence* secondo i principi generali individuati dalla Convenzione. – 3. La mutua assistenza per la formazione dell'*e-evidence* prevista dalla Convenzione sulla criminalità informatica in assenza di accordi internazionali applicabili. – 3.1. La procedura. – 4. L'oggetto della domanda di assistenza giudiziaria. – 5. L'ingiunzione di produrre. – 6. Luci ed ombre della Convenzione sulla criminalità informatica. Verso un Secondo protocollo. – 7. I lavori preparatori del Secondo protocollo. – 8. Il Secondo protocollo alla Convenzione sulla criminalità informatica. – 9. Le procedure volte a migliorare la cooperazione diretta con fornitori ed enti privati di altre Parti. Elementi di comunanza. – 9.1. La procedura per l'ottenimento di informazioni sulla registrazione del nome di dominio. – 9.2. La divulgazione delle informazioni sugli abbonati. – 10. Le nuove procedure di cooperazione internazionale tra autorità per la produzione di dati informatici. – 10.1. L'ordine di produzione accelerata. – 10.2. La divulgazione accelerata di dati informatici in assenza di una richiesta di assistenza. – 11. La mutua assistenza d'emergenza. – 12. Le regole relative alla formazione della prova elettronica transfrontaliera vigenti negli Stati Uniti d'America. – 13. I negoziati in vista di un Accordo tra l'Unione europea e gli Stati Uniti d'America.

1. La Convenzione del Consiglio d'Europa sulla criminalità informatica: un quadro generale

Tra i più importanti testi normativi che disciplinano la formazione della prova elettronica transnazionale è annoverata la Convenzione del Consiglio d'Europa sulla criminalità informatica, aperta alla firma degli Stati membri e degli Stati terzi, i quali hanno partecipato alla sua elaborazione e all'adesione degli altri Stati non membri a

Budapest il 23 novembre 2001⁵⁴⁹. La Convenzione è integrata da un protocollo aggiuntivo sulla xenofobia e il razzismo commessi tramite sistemi informatici⁵⁵⁰.

⁵⁴⁹ La Convenzione sulla criminalità informatica (STE n. 185), detta anche Convenzione di Budapest, è entrata in vigore il 1° luglio 2004. Attualmente, è stata ratificata dalla maggior parte degli Stati membri del Consiglio d'Europa, ad eccezione dell'Irlanda e della Svezia – le quali si sono limitate solo alla firma – e della Federazione Russa. È stata oggetto di ratifica da parte di molti Stati non membri, tra cui Argentina, Australia, Canada, Capo Verde, Cile, Colombia, Costa Rica, Filippine, Ghana, Giappone, Israele, Marocco, Mauritius, Panama, Paraguay, Perù, Repubblica Dominicana, Senegal, Sri Lanka, Stati Uniti d'America, Tonga, per un totale di 66 Stati. Oltre a questi, si ritiene che altri 28 Stati abbiano una legislazione largamente in linea con il trattato. Sulla convenzione, *ex multis*, E. BALAJANOV, *Setting the minimum age of criminal responsibility for cybercrime*, in *International Review of Law, Computers & Technology*, 1, 2018, p. 2 ss.; R.M.F. BARON, *A Critique of the International Cybercrime Treaty*, in *CommLaw Conspectus*, 2, 2002, p. 263 ss.; J. BESSANT, *Human Rights, the Law, Cyber-security and Democracy: After the European Convention*, in *Australian Journal of Human Rights*, 1, 2012, p. 1 ss.; D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, in *International Review of Law, Computers & Technology*, 2, 2004, p. 165 ss.; J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, in *Monash University Law Review*, 3, 2014, p. 698 ss.; P. CSONKA, *The Council of Europe Convention on Cyber-Crime: a response to the Challenge of the New Age?*, in AA.VV., *Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatica* (a cura di G. ILARDA, G. MARZULLO), Milano, 2004, p. 3 ss.; J. FISHER, *Draft Convention on Cybercrime: Potential Constitutional Conflicts*, in *University West Las Angeles Review*, 2001, p. 339 ss.; M. GERCKE, *10 years Convention on Cybercrime: Achievements and Failures of the Europe's Instrument in the Fight against Internet-related Crimes*, in *Computer Law Review International*, 5, 2011, p. 142 ss.; L. HUEY, R. ROSENBERG, *Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention*, in *Canadian Journal of Criminology and Criminal Justice*, 5, 2004, p. 597 ss.; C. JEFFRAY, T. FEAKIN, *Underground web: The cybercrime challenge*, in *Australian Strategic Policy Institute*, marzo 2015, p. 1 ss.; M. KEYSER, *The Council of Europe Convention on Cybercrime*, in *J. Transnational Law & Policy*, 2, 2003, p. 287 ss.; R.K. KNAKE, *Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity*, Council on Foreign Relations, New York, 2020, p. 1 ss.; C. LE NGUYEN, W. GOLMAN, *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "law in action"*, in *Computer Law & Security Review*, 40, 2021, Article 105521, p. 1 ss.; N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, cit., p. 699 ss.; R. MAZZA, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001*, in *La Comunità Internazionale*, 1, 2014, p. 59 ss.; M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, in *J. Mashall J. Computer & Info L.*, 2, 2005, p. 329 ss.; A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, in *Center for Cyber and Homeland Security at Auburn University*, gennaio 2018, p. 1 ss., disponibile al link: <http://www.jstor.com/stable/resrep20738>; A. PETERS, A. HINDOCHA, *US Global Cybercrime Cooperation: A Brief Explainer*, in *Third Way*, giugno 2020, p. 1 ss., disponibile al link: <https://www.jstor.org/stable/resrep25041>; M.G. PORCEDDA, *Rule of Law and Human Rights in Cyberspace*, in AA.VV., *Riding the digital wave: the impact of cyber capacity building on human development* (eds. P. PAWLAK), EU Institute for Security Studies, Paris, 2014, p. 30 ss.; C. POUNDER, *The Council of Europe Cyber-Crime Convention*, in *Computers & Security*, 5, 2001, p. 380 ss.; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, in *Dir. pen. e proc.*, 4, 2002, p. 509 ss.; E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, in *Guida al diritto*, 16, 19 aprile 2008, p. 72 ss.; ID., *Task force operativa 24 ore al giorno*, in *Guida al diritto*, 16, 19 aprile 2008, p. 74 ss.; L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, in *Computer Law & Security Review*, 24, 2018, p. 1197 ss.; Y. TURIANSKYI, *Africa and Europe: Cyber Governance Lessons*, in *South African Institute of International Affairs*, gennaio 2020, p. 10 ss., disponibile al link: <https://www.jstor.org/stable/resrep25957>; A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, in *Berkley Technology Law Journal*, 1, 2003, p. 425 ss.; D. WICKI-BIRCHLER, *The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?*, in *Int. Cybersecur. Law Rev.*, 1, 2020, p. 63 ss.

⁵⁵⁰ Cfr., Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici, (STE n.

Sebbene parte della dottrina ritiene che sia prevalentemente una legislazione simbolica⁵⁵¹, l'elevato numero di Stati non membri che l'hanno ratificata o che vi hanno aderito⁵⁵² è indice dell'enorme importanza assunta nel panorama internazionale, tanto da essere stata riconosciuta dall'Unione europea come il principale quadro multilaterale per la lotta alla criminalità informatica⁵⁵³, ed è ancora oggi ritenuta una “*gold standard*”⁵⁵⁴ per le tecniche di indagine sulla criminalità informatica grazie alla maturità manifestata a livello internazionale nella lotta a questo particolare tipo di criminalità⁵⁵⁵.

Il successo del trattato, storica pietra miliare nella lotta internazionale al *cybercrime*, è stato confermato dieci anni dopo la firma anche dal Segretario generale del Consiglio d'Europa, Thorbjørn Jagland, il quale ha affermato che la Convenzione ha dimostrato di funzionare perché ha contribuito ad un'ampia armonizzazione della legislazione relativa alla lotta alla criminalità informatica in tutto il mondo⁵⁵⁶.

La Convenzione è il primo trattato internazionale⁵⁵⁷ multilaterale vincolante sui reati commessi via internet e su altre reti informatiche, che regola in particolare le violazioni

189), aperto alla firma a Strasburgo il 28 gennaio 2003. Il Protocollo comporta un'estensione della portata della Convenzione sulla cibercriminalità, comprese le sue concrete disposizioni di cooperazione procedurali ed internazionali, per includere ugualmente i reati legati alla propaganda razzista o xenofoba. Oltre ad armonizzare gli elementi giuridici reali di tali atti, il Protocollo intende fornire alle Parti la possibilità di utilizzare i mezzi e le vie della cooperazione internazionale stabiliti nella Convenzione di Budapest in questo campo.

⁵⁵¹ Così, N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, cit., p. 702 ss., secondo la quale «*While the Convention on Cyber crime is a genuine attempt at addressing the problems of international cyber crime, the treaty remains largely a symbolic policy and thus will have a limited effect on cyber crime in the long-term. It clearly has elements of the four functions of symbolic policies*». Secondo la teoria delle *symbolic policies* – definita per la prima volta nel 1964 da Endelman – alcune politiche sono create per far avere alla popolazione la percezione di star facendo qualcosa per risolvere il problema, quando in realtà le politiche non apportano alcun cambiamento reale o significativo, né attengono alla questione specifica. Per un approfondimento sulla teoria, si rinvia a M. ENDELMAN, *The Symbolic Uses of Politics*, Chicago, 1964.

⁵⁵² Per questo motivo è ritenuta dalla dottrina una “convenzione universale”, e non poteva essere altrimenti poiché essa ha ad oggetto la «regolamentazione dell'attività informatica e la repressione delle relative attività illecite» che indubbiamente avrebbero dovuto coinvolgere la maggior parte dei soggetti del diritto internazionale. Sul punto, E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, cit., p. 72 ss.

⁵⁵³ Cfr., Comunicazione congiunta della Commissione e del vicepresidente della Commissione/Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza “Strategia dell'Unione europea per la cibersicurezza: un cberspazio aperto e sicuro”, JOIN(2013)1 final.

⁵⁵⁴ In questi termini C. JEFFRAY, T. FEAKIN, *Underground web: The cybercrime challenge*, cit., p. 3. Critico nei confronti della Convenzione, R.K. KNAKE, *Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity*, cit., p. 8, secondo il quale la Convenzione di Budapest non fornisce vantaggi tangibili ai Paesi che aderiscono, ha meccanismi deboli di coordinamento per affrontare la criminalità informatica e non indica un sistema integrato per punire gli Stati membri che non rispettano le sue regole. Mancano, inoltre, azioni che incoraggino la cooperazione.

⁵⁵⁵ In tal senso, L. LUPÀRIA, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, in *Dir. pen. e proc.*, 6, 2008, p. 717 ss.; R. MAZZA, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001*, cit., p. 59 ss.; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 509.

⁵⁵⁶ V., T. JAGLAND, *Budapest Convention on Cybercrime—10th anniversary meeting*, discorso tenuto a Strasburgo, Consiglio d'Europa, 23 novembre 2011.

⁵⁵⁷ Ai sensi dell'art. 2 della Convenzione di Vienna sul diritto dei trattati, con il termine trattato si indica un accordo internazionale concluso per iscritto tra Stati e regolato dal diritto internazionale, che sia costituito da un solo strumento o da due o più strumenti connessi, qualunque ne sia la particolare denominazione. La Convenzione di Vienna è stata conclusa a Vienna il 23 maggio 1969. In Italia è stata ratificata con l. 12 febbraio 1974, n. 112, in GU 30 aprile 1974, n. 111, ed è in vigore dal 27 gennaio 1980. Sul tema, R. AGO, *Droit des traités à la lumière de la Convention de Vienne*, in *Collected Courses of the*

dei diritti d'autore, la frode informatica, la pornografia minorile e le violazioni della sicurezza della rete⁵⁵⁸. Contiene, inoltre, un ventaglio di misure e procedure appropriate, quali la perquisizione dei sistemi di reti informatiche e l'intercettazione dei dati. Infine, ampio spazio è dedicato ai meccanismi di cooperazione internazionale per la lotta ai crimini collegati ai sistemi informatici e ai dati informatici o per la formazione delle prove, in forma elettronica, di un reato, facendo obbligo alle parti di definire i poteri e le procedure per ottenere prove elettroniche e prestarsi assistenza giudiziaria, non solo in relazione ai reati informatici.

La necessità di una simile normativa emerse già nel 1995 con la raccomandazione n. 13 del Consiglio d'Europa⁵⁵⁹, ove si prestò attenzione non solo ai problemi di diritto sostanziale e processuale connessi all'informatica ed alla digitalizzazione, ma soprattutto al necessario coordinamento investigativo tra gli Stati membri del Consiglio d'Europa⁵⁶⁰.

Hague Academy of International Law, 3, 1971, p. 303 ss.; F. CAPOTORTI, *Il diritto dei trattati secondo la Convenzione di Vienna*, in *Convenzione di Vienna sul diritto dei trattati*, Padova, 1969, p. 11 ss.; B. CONFORTI, *Diritto internazionale*, Napoli, 2014, p. 71 ss.; O. CORTEN, P. KLEIN, *The Vienna Conventions on the Law of Treaties: a Commentary*, 2 voll., Oxford, 2011, *passim*; O. DÖRR, K. SCHMALENBACH, *Vienna Convention on the Law of Treaties: a Commentary*, Heidelberg, 2012, *passim*; T.O. ELIAS, *The Modern Law of Treaties*, Leiden, 1974, *passim*; A. HARATSCH, S. SCHMAHL, *Die Anwendung ratione temporis der Wiener Konvention über das Recht der Verträge*, in *Zeitschrift für Öffentliches Recht*, 2003, p. 105 ss.; U. LINDERFALK, *On the Interpretation of Treaties: the Modern International Law as Expressed in the 1969 Vienna Convention on the Law of Treaties*, Dordrecht, 2007, *passim*; A. ORAKHELASHVILI, S. WILLIAMS (eds.), *40 Years of the Vienna Convention on the Law of Treaties*, London, 2010; A. SINAGRA, P. BARGIACCHI, *Lezioni di diritto internazionale pubblico*, cit., p. 182 ss.; M.E. VILLIGER, *Commentary on the 1969 Vienna Convention on the Law of Treaties*, Leiden, 2009, *passim*; ID., *The 1969 Vienna Convention on the Law of Treaties: 40 Years after*, in *Collected Courses of the Hague Academy of International Law*, 2009, p. 9 ss.

⁵⁵⁸ Oltre alla Convenzione sulla criminalità informatica, nel tempo sono stati conclusi altri trattati aventi ad oggetto la stessa materia. Ad esempio, nel 2001 è stato siglato l'accordo di cooperazione della Comunità degli Stati indipendenti per la lotta ai reati relativi all'informatica; nel 2010 è stata sottoscritta la Convenzione della Lega degli Stati Arabi sulla lotta contro i reati legati alle tecnologie dell'informazione, mentre, nel 2014 è stata firmata la Convenzione dell'Unione africana sulla sicurezza informatica e la protezione dei dati personali (nota anche come Convenzione di Malabo).

⁵⁵⁹ La Raccomandazione n. R (95) 13 del Consiglio dei Ministri agli Stati membri relativa ai problemi di procedura penale legati alla tecnologia dell'informazione (adottata dal Consiglio dei Ministri l'11.9.1995, nel corso della 543^a riunione dei Delegati dei Ministri) aveva per la prima volta notato che le leggi di procedura penale degli Stati membri non prevedevano ancora poteri appropriati né per eseguire perquisizioni all'interno dei sistemi informatici né per ricercare elementi aventi attitudine probatoria nel corso delle inchieste penali. Inoltre, non esisteva un meccanismo di cooperazione internazionale per la formazione delle prove elettroniche transfrontaliere compatibile con le leggi di procedura penale in materia. Pertanto, si paventava il rischio che gli Stati membri non fossero in grado di fornire collaborazione giudiziaria adeguata in caso di richiesta di raccolta di prove elettroniche, sul loro territorio, all'interno di sistemi elettronici d'informazione. Per un richiamo, E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, cit., p. 72 ss.

⁵⁶⁰ L'iter che avrebbe portato alla Convenzione sulla criminalità informatica comincia nel novembre 1996 con la decisione CDPC / 103/211196 del Comitato europeo per i problemi della criminalità (CDPC) di istituire un comitato di esperti per affrontare la criminalità informatica. Nelle motivazioni della decisione emerge con chiarezza la volontà del Comitato di addivenire ad una Convenzione sul rilievo che l'integrazione dei sistemi di telecomunicazione e di informazione, che consente l'archiviazione e la trasmissione, indipendentemente dalla distanza, di tutti i tipi di comunicazione apre una vasta gamma di nuove possibilità. Questi sviluppi sono stati stimolati dall'emergere di super-autostrade e reti informatiche, compreso Internet, attraverso le quali praticamente chiunque potrà avere accesso a qualsiasi servizio di informazione elettronica indipendentemente da dove si trova nel mondo. Grazie ai servizi di comunicazione e informazione gli utenti creano una sorta di spazio comune, chiamato "cyber-spazio", che viene utilizzato per scopi legittimi ma può anche essere oggetto di abuso. Questi reati commessi contro l'integrità, la

Obiettivo principale della Convenzione, enunciato nel preambolo, è perseguire una politica penale comune per la protezione della società contro la criminalità informatica,

disponibilità, e la riservatezza dei sistemi informatici e delle reti di telecomunicazione o consistenti nell'uso di tali reti dei loro servizi per commettere reati tradizionali si caratterizzano per transnazionalità.

Secondo il Comitato, il diritto penale deve quindi tenersi al passo con gli sviluppi tecnologici che offrono opportunità altamente sofisticate per abusare delle strutture del cyber-spazio e arrecare danno a interessi legittimi. Data la natura transfrontaliera delle reti di informazione, è stato ritenuto necessario uno sforzo internazionale concertato per far fronte a tale abuso. Sebbene la Raccomandazione n. (89) 9 abbia portato ad un ravvicinamento dei concetti nazionali riguardanti alcune forme di uso improprio dei computer, solo uno strumento internazionale vincolante può garantire la necessaria efficienza nella lotta contro questi nuovi fenomeni. Pertanto, il Comitato invitava ad affrontare questioni relative alle misure di cooperazione internazionale, di diritto sostanziale e procedurale, nonché quelle strettamente connesse con l'uso della tecnologia dell'informazione.

Inoltre, il CDPC ha tenuto conto della Relazione, redatta - su sua richiesta - dal Prof. H.W.K. Kaspersen, che ha concluso che «dovrebbe essere considerato un altro strumento giuridico con più impegno di una raccomandazione, come una convenzione. Tale convenzione non dovrebbe occuparsi solo di questioni di diritto penale sostanziale, ma anche di questioni procedurali penali e di procedure e accordi di diritto penale internazionale», osservazione già emersa dalla Relazione allegata alla Raccomandazione n. R (89) 9 sul diritto sostanziale e dalla Raccomandazione n. R (95) 13 sui problemi di diritto processuale connessi alla tecnologia dell'informazione.

A seguito della decisione del CDPC, il Comitato dei Ministri ha istituito un nuovo comitato, denominato "Comitato di esperti sulla criminalità nel cyber-spazio (PC-CY: Committee of Experts on Crime in Cyberspace)" con decisione n. ° CM / Del / Dec (97) 583, presa alla 583a riunione dei Delegati dei Ministri (tenutasi il 4 febbraio 1997). Il comitato PC-CY ha iniziato i suoi lavori nell'aprile 1997 e ha avviato i negoziati su un progetto di convenzione internazionale sulla criminalità informatica. Secondo il suo mandato originale, il Comitato doveva terminare i suoi lavori entro il 31 dicembre 1999. Poiché a quella data il Comitato non era ancora in grado di concludere pienamente i suoi negoziati su alcune questioni nel progetto di Convenzione, i termini furono prorogati con decisione n. CM / Del / Dec (99) 679 dei delegati dei ministri al 31 dicembre 2000. I ministri europei della giustizia hanno espresso il loro sostegno due volte in merito ai negoziati: con la risoluzione n. 1, adottata alla loro 21a conferenza (Praga, giugno 1997), la quale ha raccomandato al Comitato dei Ministri di sostenere il lavoro svolto dal CDPC sulla criminalità informatica al fine di ravvicinare le disposizioni del diritto penale interno e consentire l'uso di mezzi di indagine efficaci su tali reati; con la Risoluzione n. ° 3, adottata alla 23a Conferenza dei Ministri Europei della Giustizia (Londra, giugno 2000), la quale ha incoraggiato le parti negoziali a proseguire i loro sforzi al fine di trovare soluzioni adeguate in modo da consentire al maggior numero possibile di Stati di diventare Parti alla Convenzione e ha riconosciuto la necessità di un sistema rapido ed efficiente di cooperazione internazionale, che tenga debitamente conto delle esigenze specifiche della lotta alla criminalità informatica. Gli Stati membri dell'Unione europea hanno espresso il loro sostegno al lavoro del PC-CY attraverso una posizione comune, adottata nel maggio 1999.

Dopo la pubblicazione di una serie di bozze, al fine di consentire agli Stati negoziatori di consultarsi con tutte le parti interessate, il progetto di Convenzione rivisto e il suo *Memorandum* esplicativo sono stati sottoposti all'approvazione del CDPC nella sua 50a sessione plenaria nel giugno 2001, a seguito della quale il testo del progetto di Convenzione è stato sottoposto al Comitato dei Ministri. Il 7 Novembre 2001 il Comitato l'adottava, aprendo la Convenzione alla firma il 23 novembre 2001, in occasione della Conferenza sul *cibercrime*, tenutasi a Budapest il giorno precedente. V., per una ricostruzione storica, R.M.F. BARON, *A Critique of the International Cybercrime Treaty*, cit., p. 265 ss.; J. BESSANT, *Human Rights, the Law, Cyber-security and Democracy: After the European Convention*, cit., p. 6 ss.; P. CSONKA, *The Draft Council of Europe Convention on Cyber-Crime: a Response to the Challenge of Crime in the Age of the Internet?*, in *Computer Law & Security Report*, 5, 2000, p. 329 ss.; C. JEFFRAY, T. FEAKIN, *Underground web: The cybercrime challenge*, cit., p. 5 ss.; C. LE NGUYEN, W. GOLMAN, *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "law in action"*, cit., p. 2 ss.; N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, cit., p. 699 ss.; M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, cit., p. 333 ss.; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 509 ss.; A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, cit., p. 428 ss.

invitando gli Stati a adottare una legislazione interna adeguata alle nuove sfide della tecnologia e a sviluppare una cooperazione internazionale in grado di far fronte ai profondi cambiamenti dipendenti dall'introduzione della tecnologia digitale e dalla convergente e costante globalizzazione delle reti informatiche⁵⁶¹.

Siccome le reti informatiche e le informazioni in formato elettronico aumentano il rischio di fatti riprovevoli quali la commissione di reati o la dispersione e genuinità delle prove connesse a questi ultimi, la Convenzione ha concretamente intercettato la necessità di una cooperazione facile e veloce tra Stati, nonché tra questi ultimi e società private, che faciliti l'individuazione dei reati, le indagini e l'esercizio dell'azione penale a livello sia nazionale sia internazionale, garantendo, al contempo, sia gli interessi legittimi nell'uso e nello sviluppo delle tecnologie informatiche, sia i diritti e le libertà individuati nella Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, mediante un equo bilanciamento tra azione repressiva e rispetto dei diritti umani⁵⁶².

Emerge, quindi, un modello che concilia la visione di un internet libero – dove le informazioni possono fluire senza impedimenti ed essere accessibili e condivise – con la necessità di una risposta efficace della giustizia penale alla criminalità. Le restrizioni sono strettamente definite: sono previsti e perseguibili solo specifici reati e possono essere prova solo determinati dati ritenuti necessari nei procedimenti penali, nel pieno rispetto delle garanzie relative ai diritti umani ed allo stato di diritto⁵⁶³.

Generalmente, è accettata l'idea che un determinato grado di armonizzazione tra i Paesi sia vitale se si vuole ottenere una disciplina efficace per la lotta ai crimini informatici. L'armonizzazione generata dalla Convenzione sulla criminalità informatica è ritenuta essenziale per due ragioni.

Innanzitutto, elimina o riduce l'incidenza di “rifugi”, ossia di aree non disciplinate ed in cui non è possibile agire in funzione repressiva nel caso di commissione di fatti

⁵⁶¹ Gli scopi della convenzione sono così riassumibili: armonizzare gli elementi dei reati previsti dai singoli ordinamenti nazionali e le disposizioni comuni in materia di cibercriminalità; fornire al diritto processuale nazionale i poteri necessari al perseguimento dei reati di questo tipo di crimine, così come di altre infrazioni commesse mediante un sistema informatico o nel quadro dei quali esistono prove sotto forma elettronica; sviluppare un sistema rapido ed efficace di cooperazione internazionale. V., in tal senso, D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, cit., p. 166; J. FISHER, *Draft Convention on Cybercrime: Potential Constitutional Conflicts*, cit., p. 343 ss.; S. FURNELL, *Cyber crime: Vandalizing the Information Society*, Boston, 2002; N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, cit., p. 701 ss.; M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, cit., p. 329 ss.; A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, cit., p. 12, disponibile al link: <http://www.jstor.com/stable/resrep20738>; E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, cit., p. 72 ss.; L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, cit., p. 1198; D. WICKI-BIRCHLER, *The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?*, cit., p. 65.

⁵⁶² Nel preambolo, particolare attenzione è destinata anche alla Convenzione internazionale delle Nazioni Unite del 1966 sui Diritti Civili e Politici e agli altri diritti umani che riaffermano il diritto di ciascuno di avere opinioni senza condizionamenti, come ad esempio il diritto alla libertà di espressione, incluso il diritto di cercare, ricevere e trasmettere informazioni e idee di ogni tipo, senza limiti di frontiere, e il diritto al rispetto della privacy. Sono menzionate anche la Convenzione del 1981 del Consiglio d'Europa per la tutela degli Individui con riguardo alla gestione automatizzata dei dati personali; la Convenzione delle Nazioni Unite del 1989 sui diritti dei minori; la Convenzione del 1999 dell'Organizzazione Internazionale del Lavoro sulle peggiori forme di lavoro minorile; la Convenzione del Consiglio d'Europa sulla cooperazione in materia penale.

⁵⁶³ In tal senso, CYBERCRIME CONVENTION COMMITTEE (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, T-CY (2020)16, Strasburgo, 2020, p. 4.

talmente riprovevoli da dover richiedere un intervento sanzionatorio di tipo penale. Infatti, se la condotta non è criminalizzata in uno specifico Paese, le persone in quel territorio possono agire impunemente commettendo reati che possono interessare altre giurisdizioni. Inoltre, una carenza di armonizzazione potrebbe rivelarsi deleteria per la formazione della prova sino al punto da vanificare qualsiasi sforzo profuso nella raccolta. Da ciò se ne ricava anche il secondo e più importante motivo: l'armonizzazione si rivela fondamentale per una efficace cooperazione tra le forze dell'ordine⁵⁶⁴.

In Italia, la Convenzione di Budapest è stata ratificata con l. 18 marzo 2008, n. 48, la quale ha introdotto per la prima volta una disciplina specifica in tema di assunzione degli elementi di prova digitali attraverso la modifica degli articoli in materia di perquisizione, sequestro, acquisizione e conservazione dei dati contenuti su supporti informatici⁵⁶⁵, intervenendo in modo corposo sull'impianto codicistico.

⁵⁶⁴ Sul punto, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 700 ss.

⁵⁶⁵ Il legislatore ha recepito la Convenzione di Budapest con sette anni di ritardo. È stata utilizzata una tecnica legislativa "aperta" che consente di stabilire obiettivi generali quali la genuinità e la non alternazione del dato informatico, senza indicare le procedure da seguire. In tal modo si permette l'impiego delle *best practice* internazionali più aggiornate, ma d'altra parte non consente di risolvere tutti i problemi interpretativi sorti nella pratica. Sulle modifiche apportate dalla l. 18 marzo 2008, n. 48, v., tra i tanti, S. ATERNO, *La Convenzione di Budapest del 2001 e la l. n. 48/2008*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1351 ss.; ID., voce *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen.*, cit., p. 217 ss.; ID., sub art. 8, in AA.VV., *Cybercrime, responsabilità degli enti, prova digitale* (a cura di G. CORASANITI, G. CORRIAS LUCENTE), Padova, 2009, p. 194 ss.; A. BARBIERI, *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici (commento a l. 18 marzo 2008, n. 48)*, in *Diritto dell'internet*, 5, 2008, p. 516 ss.; L. BARTOLI, C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, 1-2, 2015, p. 139 ss.; M.L. DI BITONTO, A. VITALE, A. MACRILLÒ, A. BARBIERI, E. FORLANI, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, in *Diritto dell'internet*, 5, 2008, p. 503 ss.; F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono...*, in *Cyberspazio e diritto*, 1, 2010, p. 185 ss.; L. CORDÌ, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 8*, in *Leg. Pen.*, 2008, p. 286 ss.; G. COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Cyberspazio e diritto*, 3, 2010, p. 465 ss.; G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 9*, in *Leg. Pen.*, 2008, p. 297 ss.; M.L. DI BITONTO, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, cit., p. 503 ss.; I.V. FELCHER, *Una rassegna giurisprudenziale con riferimento alla Legge n. 48 del 2008 e alle investigazioni digitali*, in *Cyberspazio e diritto*, 1, 2013, p. 131 ss.; E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in AA.VV., *Sistema penale e criminalità informatica* (a cura di L. LUPARIA), Milano, 2009, p. 143 ss.; L. LUPARIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul Cybercrime*, in AA.VV., *Le nuove norme sulla sicurezza pubblica* (a cura di S. LORUSSO), Padova, 2008, p. 63 ss.; ID., *La ratifica della Convenzione cybercrime del Consiglio d'Europa. Profili processuali*, cit., p. 717 ss.; D. MANZIONE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 11 – Competenza*, in *Leg. Pen.*, 2008, p. 314 ss.; L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4509B ss.; S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2, 2015, p. 760C; F.M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, cit., p. 696B ss.; A. MONTI, *La nuova disciplina del sequestro informatico*, in AA.VV., *Sistema penale e criminalità informatica* (a cura di L. LUPARIA), Milano, 2009, p. 207 ss.; L. PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 5, 2008, p. 437 ss.; ID., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 6, 2008, p. 700 ss.; M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., *passim*; F. RESTA, *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 9, 2008, p. 2147B ss.; P. RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 4, 2013, p. 1691B; C. SARZANA DI SANT'IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Criminalità informatica*, 12, 2008, p. 1562 ss.; E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, cit., p. 72 ss.; P. TONINI, *Documento informatico e giusto*

La qualità dell'attuazione è valutata dal Comitato della Convenzione sulla criminalità informatica (T-CY) che rappresenta le Parti della Convenzione di Budapest, con i firmatari e gli Stati invitati ad aderire come osservatori. Inoltre, gli Stati impegnati a cooperare ai sensi della presente Convenzione sono sostenuti con progetti di rafforzamento delle capacità gestiti da un apposito Ufficio per il programma sulla criminalità informatica del Consiglio d'Europa (C-PROC), con sede in Romania.

Un ruolo di primaria importanza è ricoperto infine dal Comitato Europeo per i Problemi Criminali (CDPC)⁵⁶⁶. La Convenzione è particolarmente attenta a ipotesi patologiche come possibili contrasti tra Parti contraenti ed incentiva il dialogo tra questi. In tali casi, il CDPC è coinvolto in quanto organo di supervisione e controllo.

Ai sensi dell'art. 45 della Convenzione, esso deve essere informato dell'interpretazione e dell'applicazione della stessa. In caso di contrasto tra Stati sull'interpretazione e sull'applicazione della Convenzione, le Parti attiveranno un negoziato o altro strumento pacifico di risoluzione della controversia a loro scelta. Tra questi rimedi alternativi, rientra la sottoposizione del contrasto al Comitato Europeo per i Problemi Criminali. Altri due meccanismi suggeriti sono la sottoposizione del contrasto a un tribunale arbitrale o alla Corte Internazionale di Giustizia.

Si incentiva il confronto diretto tra gli Stati e una diligente organizzazione sotto l'egida del CDPC. Invero, l'art. 46 della Convenzione prescrive che le Parti si consultino periodicamente al fine di facilitare: l'effettivo uso e l'esecuzione della Convenzione, «inclusa l'individuazione di ogni problema in materia, così come gli effetti di ogni dichiarazione o riserva fatta riguardo alla presente Convenzione»; lo scambio di informazioni sugli sviluppi legislativi, politici o tecnologici riguardanti la criminalità informatica e la raccolta di prove in formato elettronico; la valutazione di eventuali integrazioni o emendamenti della Convenzione. In tale contesto, il CDPC è costantemente informato ed assume, all'occorrenza, un ruolo di facilitatore dei colloqui.

La procedura, ordunque, appare particolarmente flessibile poiché lascia la possibilità in capo alle Parti di decidere tempi e luoghi della convocazione, ma al tempo stesso preserva il ruolo di garanzia e controllo assunto dal CDPC, il quale non solo sarà regolarmente informato delle consultazioni che hanno luogo tra le Parti, ma le agevolerà e adotterà ogni misura necessaria per assistere le Parti nei loro sforzi per completare o modificare la Convenzione⁵⁶⁷.

Data l'importanza della Convenzione, ci si sarebbe aspettato una precisa definizione di prova elettronica, indispensabile per il contesto in cui si opera. Invece, seppur la Convenzione, limitatamente ad essa, dedichi l'intero art. 1 alle definizioni di alcuni

processo, in *Dir. pen. e proc.*, 4, 2009, p. 401 ss.; M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008*, n. 48, in *Informatica e diritto*, 1-2, 2015, p. 65 ss.; N. VENTURA, *Ratifica della Convenzione di Budapest e iniziativa investigativa della polizia giudiziaria*, in *Giust. pen.*, 1, 2008, p. 226 ss.; A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. dell'internet*, 5, 2008, p. 507 ss.

⁵⁶⁶ Il Comitato europeo per i problemi del crimine (CDPC) è stato istituito nel 1958 e si riunisce presso la sede del Consiglio d'Europa a Strasburgo (Francia). È incaricato dal Comitato dei Ministri di supervisionare e coordinare le attività del Consiglio d'Europa nel campo della prevenzione e del controllo della criminalità. Il CDPC individua le priorità per la cooperazione giuridica intergovernativa, formula proposte al Comitato dei Ministri sulle attività nei settori del diritto e della procedura penale, della criminologia e della penologia e implementa queste attività. Inoltre, elabora convenzioni, raccomandazioni e rapporti. Organizza conferenze di ricerca criminologica e colloqui criminologici, conferenze dei direttori dell'amministrazione penitenziaria.

⁵⁶⁷ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 328, p. 60.

termini tecnici di stretta attinenza all'ambito informatico, né la Convenzione sulla criminalità informatica, né la Raccomandazione R(95) 13 ne tracciano con precisione i contorni, limitandosi solo a menzionarla⁵⁶⁸.

Al di là di tale aspetto, è l'assetto strutturale assunto dalla Convenzione a regalare all'interprete particolari spunti di riflessione sugli obiettivi ad "ampio spettro" che essa vuole perseguire. Non si è voluto solo armonizzare gli elementi del diritto penale sostanziale interno in relazione ai reati e alle disposizioni collegate nel settore della criminalità informatica, ma si è pensato anche di fornire le competenze di diritto procedurale penale a livello interno necessarie per le indagini e per l'esercizio dell'azione penale in relazione a tali reati, così come in relazione ad altri reati commessi per mezzo di un sistema informatico o a prove in formato elettronico aventi ad oggetto fatti di reato del tutto sganciati dal contesto tecnologico ed informatico⁵⁶⁹, nonché a istituire un regime di cooperazione internazionale rapido ed efficiente.

È chiaro, allora, che la Convenzione non vuole rivolgersi solo all'ampio settore della criminalità informatica, intesa come quel fenomeno che si manifesta con reati informatici o commessi per mezzo di sistemi informatici, ma anche all'ormai imperante mondo della formazione di prove elettroniche di reati i cui elementi strutturali prescindono da aspetti informatici. Di talché, la Convenzione assume una sua funzione anche in relazione a reati i cui unici profili informatici sono individuabili esclusivamente nella prova. Infatti, è innegabile come nel contesto attuale la *digital evidence* assuma un ruolo di primo piano nella formazione della verità processuale⁵⁷⁰, che consenta al giudice ed alle parti di costruire una spiegazione ragionevole e razionale al fatto in esame.

Invero, l'ambito di operatività delle norme della Convenzione sulla criminalità informatica è individuato secondo un criterio oggettivo ed un criterio teleologico, laddove secondo il criterio oggettivo le norme della Convenzione si applicano per la repressione delle condotte illecite compiute contro o per mezzo del sistema informatico, mentre il criterio teleologico consente di applicare la disciplina prevista dalla Convenzione per la ricerca e la conservazione delle prove elettroniche di qualsiasi reato⁵⁷¹.

⁵⁶⁸ Ci si riferisce alla definizione di sistema informatico, inteso quale «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati»; di dati informatici, ossia «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione»; di *service provider*, cioè il fornitore di servizi, il quale può essere «qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico» o comunque «qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio»; di trasmissione di dati, il quale indica «qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio».

⁵⁶⁹ La dottrina ha evidenziato come siano sempre più numerosi i reati che lasciano una semplice "traccia elettronica" in computer o supporti informatici. Da qui, l'inevitabile espansione di nuove tecniche investigative e della necessaria formulazione di una nuova disciplina processuale, attualmente solo in parte sviluppatasi. In tal senso, L. PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, cit., p. 448. Sul punto, anche, L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa: i profili processuali*, cit., p. 717.

⁵⁷⁰ Così, L. LUPARIA, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa: i profili processuali*, cit., p. 717.

⁵⁷¹ In tal senso, S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il secondo Protocollo addizionale alla Convenzione di Budapest*, in *Dir. pen. proc.*, 8, 2021, p. 1032. V., inoltre, F. GRAZIANI, *L'acquisizione della prova digitale all'estero: verso un secondo Protocollo addizionale alla*

La Convenzione si compone di un preambolo e quattro capitoli⁵⁷², per un totale di 48 articoli. Il capitolo I è dedicato alle definizioni; il capitolo II contiene i provvedimenti da adottare a livello nazionale; il capitolo III disciplina la cooperazione internazionale; il capitolo IV indica le disposizioni finali.

Di questi, il capitolo II è suddiviso in tre sezioni. La sezione I si occupa del diritto penale sostanziale e copre sia disposizioni in materia di criminalità informatica sia disposizioni connesse alla criminalità informatica: dapprima definisce nove reati⁵⁷³ raggruppati in diverse categorie; poi si occupa delle altre forme di responsabilità – tra cui quella delle persone giuridiche – e delle sanzioni. La sezione II sul diritto procedurale penale ha una portata che va ben oltre i reati definiti nella sezione I, in quanto si applica a qualsiasi reato commesso per mezzo di un sistema informatico o le cui prove sono in forma elettronica. In esso si determinano le condizioni e le garanzie comuni applicabili a tutti gli istituti procedurali disciplinati⁵⁷⁴, tra cui l'ordine di produzione (art. 18), altrimenti detto ingiunzione a produrre, la conservazione rapida dei dati informatici immagazzinati (art. 16), la conservazione e divulgazione rapide di dati relativi al traffico (art. 17), la perquisizione e il sequestro dei dati informatici immagazzinati (art. 19), la raccolta in tempo reale dei dati sul traffico (art. 20), l'intercettazione di dati relativi al contenuto (art. 21). La sezione III, composta dal solo art. 22, disciplina la competenza, da non intendersi in senso squisitamente tecnico, ma come equivalente della nozione di "giurisdizione" dell'ordinamento italiano.

Il capitolo III contiene le disposizioni in materia di assistenza giudiziaria tradizionale e connessa alla criminalità informatica, nonché le norme sull'estradizione. Due sono le ipotesi in cui la mutua assistenza tradizionale è disciplinata: situazioni in cui sia assente una base giuridica (trattato, legislazione reciproca, ecc.) tra le parti, nel qual caso si applicano le disposizioni della Convenzione; situazioni in cui esiste una base giuridica, nel qual caso le disposizioni della Convenzione si applicano in conformità alle norme già esistenti relative all'assistenza.

L'assistenza specifica contro la criminalità informatica è disciplinata alla sezione II. Si applica sia in presenza sia in assenza di una base giuridica tra le parti e copre la stessa

Convenzione di Budapest sul cybercrime, in AA.VV., *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa* (a cura di S. MARCHISIO, U. MONTUORO), Torino, 2019, p. 56.

⁵⁷² Sulla struttura della convenzione, anche, D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, cit., p. 166 ss.; J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 702 ss.; J. FISHER, *Draft Convention on Cybercrime: Potential Constitutional Conflicts*, in *University West Las Angeles Review*, cit., p. 344 ss.; C. JEFFRAY, T. FEAKIN, *Underground web: The cybercrime challenge*, cit., p. 5 ss.; C. LE NGUYEN, W. GOLMAN, *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "law in action"*, cit., p. 3 ss.; N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, cit., p. 699 ss.; M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, cit., p. 336 ss.; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 510 ss.; A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, cit., p. 430 ss.

⁵⁷³ I reati sono i seguenti: accesso illegale ad un sistema informatico (art. 2); intercettazione abusiva (art. 3); attentato all'integrità dei dati (art. 4); attentato all'integrità di un sistema (art. 5); abuso di apparecchiature (art. 6); falsificazione informatica (art. 7); frode informatica (art. 8); reati relativi alla pornografia minorile (art. 9); reati contro la proprietà intellettuale e diritti collegati (art. 10).

⁵⁷⁴ Si tratta della conservazione rapida dei dati informatici immagazzinati, della conservazione e divulgazione rapide di dati relativi al traffico, dell'ordine di produzione internazionale (ingiunzione di produrre), della perquisizione e sequestro dei dati informatici, della raccolta in tempo reale dei dati sul traffico, dell'intercettazione di dati relativi al contenuto.

gamma di istituti procedurali definiti nel Capitolo II, fatte salve ulteriori o eccezionali condizioni. Inoltre, il capitolo III contiene una disposizione su un tipo specifico di accesso transfrontaliero ai dati informatici archiviati che non richiede assistenza reciproca (con il consenso o laddove disponibile pubblicamente) e prevede la creazione e l'operatività di una rete 24 ore su 24, 7 giorni su 7 per garantire una rapida assistenza tra gli Stati.

Infine, il capitolo IV contiene le clausole finali, che - con alcune eccezioni - ripetono le disposizioni standard dei trattati del Consiglio d'Europa.

2. La mutua assistenza per la formazione dell'*e-evidence* secondo i principi generali individuati dalla Convenzione

Il capitolo III della Convenzione del Consiglio d'Europa sulla criminalità informatica è totalmente dedicato alla cooperazione internazionale. Gli Stati sono consapevoli che una delle migliori modalità di lotta alla criminalità informatica è la collaborazione tra loro.

Invero, se da un lato le nuove tecnologie hanno consentito l'accelerazione dei traffici ed un importante progresso sociale, culturale, tecnologico e scientifico, dall'altro inevitabilmente hanno permesso l'evoluzione di nuove forme di criminalità.

Una seria lotta alla criminalità transfrontaliera – non solo di tipo informatico – è possibile solo attraverso l'evoluzione di un capillare e centrale sistema di cooperazione tra Stati, sempre più consapevoli che i nuovi fenomeni criminogeni trovano il proprio *humus* in uno spazio senza confini come il *cyberspace*.

Tale posizione emerge con forza già dal Preambolo alla Convenzione, nel quale si afferma che gli Stati parte sono convinti della necessità di proteggere la società dalla criminalità informatica mediante lo sviluppo la cooperazione internazionale, «tenendo presente la Convenzione del Consiglio d'Europa sulla cooperazione in campo penale ed anche i trattati simili che esistono tra gli Stati membri del Consiglio d'Europa e gli altri Stati» ed evidenziando che la Convenzione di Budapest è intesa quale «integrazione di queste convenzioni al fine di rendere più efficienti le indagini e l'azione penale su reati commessi in materia di sistemi informatici ed informazioni e consentire la raccolta di prove di un reato in forma elettronica»⁵⁷⁵.

Da ciò, se ne ricava la funzione servente e sussidiaria alle altre convenzioni relativa alla cooperazione in materia penale. Sembra così evidente l'annoso dilemma che si prospetta innanzi all'interprete ogni volta che si trovi ad operare in un contesto transazionale: qual è la fonte normativa e lo strumento non solo corretto ma anche più idoneo da utilizzare?

In particolare, ancora oggi le indagini informatiche aventi ad oggetto la formazione di prove digitali collocate in un territorio straniero sono svolte ricorrendo ai classici strumenti della cooperazione giudiziaria, in assenza di una normativa internazionale

⁵⁷⁵ V., *Preambolo* alla Convenzione del Consiglio d'Europa sulla criminalità informatica. Inoltre, l'art. 39 della stessa Convenzione esplicita lo scopo di completare i trattati e gli accordi bilaterali e multilaterali applicabili, esistenti tra le parti, incluse le disposizioni della Convenzione europea sull'estradizione, aperta alla firma a Parigi, il 13 dicembre 1957 (ETS n. 24), della Convenzione europea sulla mutua assistenza in campo penale, aperta a Strasburgo, il 20 aprile 1959 (ETS n. 30) e il Protocollo addizionale della Convenzione europea sulla mutua assistenza in campo penale, aperto alla firma a Strasburgo, il 17 marzo 1978 (ETS n. 99).

unificata per tutti gli Stati, tale da fissare criteri giuridici e protocolli tecnici comuni⁵⁷⁶. Per la formazione della prova elettronica, alle convenzioni bilaterali e multilaterali di assistenza giudiziaria, si affianca la Convenzione di Budapest e, per l'Italia, la disciplina prevista in via residuale nel libro XI, agli artt. 696 ss. c.p.p.⁵⁷⁷

In ogni caso, ogni fonte non vive come una monade nel proprio mondo, né esiste una “monade dominante” rispetto alle altre, sicché le fonti internazionali si integrano tra loro e, per quanto non previsto o in quanto non dispongano diversamente, con le prescrizioni sussidiarie degli artt. 696 ss. c.p.p.

Giova sottolineare che l'art. 2, l. 18 marzo 2008, n. 48, rubricato “ordine di esecuzione”, dispone la piena e intera esecuzione della Convenzione sulla criminalità informatica, in conformità a quanto disposto dall'art. 36 della Convenzione stessa. Pertanto, per gli artt. da 25 a 29 e da 31 a 34 della Convenzione non è stato necessario adottare ulteriori misure legislative⁵⁷⁸.

Il capitolo III si apre con i principi generali alla cooperazione internazionale e traccia sia quelli relativi alla procedura *in personam*, sia quelli relativi alle procedure *in rem* relativi alla mutua assistenza ed alle informazioni spontanee⁵⁷⁹.

L'art. 23⁵⁸⁰ indica tre principi generali relativi alla cooperazione internazionale: il principio dell’“ampia collaborazione”; il principio di estensione alla criminalità comune; il principio di conformità.

Il principio di ampia collaborazione chiarisce che la cooperazione internazionale deve essere fornita tra le Parti «nella misura più ampia possibile», con ciò richiedendo alle Parti di fornire una cooperazione reciproca vasta e di ridurre al minimo gli ostacoli al flusso

⁵⁷⁶ In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1621 ss.

⁵⁷⁷ Inoltre, come chiarito dall'art. 39, par. 2, della Convenzione sulla criminalità informatica «Qualora due o più Parti abbiano già concluso un accordo o un trattato sulla materia trattata dalla presente Convenzione o abbiano in altro modo regolato le proprie relazioni su tali materie, o dovessero farlo in futuro, esse avranno anche facoltà d'applicare tale accordo o trattato o regolare le loro relazioni di conseguenza, in luogo della presente Convenzione. Tuttavia, qualora le Parti stabiliscano le loro relazioni relative alle materie trattate nella presente Convenzione in modo diverso, esse dovranno farlo in modo che non sia incompatibile con l'oggetto e i principi della Convenzione».

⁵⁷⁸ Il dato è recuperabile dal prospetto informativo *Cybercrime legislation Domestic equivalent to the provisions of the Budapest Convention* relativo all'Italia del 1° maggio 2020 e redatto dall'*Octopus Cybercrime Community* del Consiglio d'Europa e rinvenibile al seguente link: <https://rm.coe.int/octocom-legal-profile-italy/16809e59c9>.

⁵⁷⁹ Cfr., D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, cit., p. 171; J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 705; M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 315 ss.; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 511; E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, cit., p. 72 ss.; A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, cit., p. 433 ss.

⁵⁸⁰ L'art. 23 recita: «Le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale». In tema, C. LE NGUYEN, W. GOLMAN, *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: “Law on the books” vs “law in action”*, cit., p. 3; A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, cit., p. 14 ss.; L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, cit., p. 1208.

regolare e rapido di informazioni e prove a livello internazionale⁵⁸¹. Si ritiene anche che esprima un *favor* verso un dialogo franco e sincero tra le Parti, al fine di superare eventuali impedimenti all'esecuzione della rogatoria.

La norma non prevede espressamente il principio di reciprocità⁵⁸², ma individua un principio che indica una condotta di massima, senza soffermarsi sul *quantum* o comunque sul livello minimo di cooperazione che il singolo Stato debba garantire, in linea con i criteri del principio strutturale della mutua assistenza, demandandolo implicitamente alla discrezionalità delle autorità nazionali.

Con il principio di estensione alla criminalità comune, la Convenzione scioglie le proprie briglie, rivolgendosi anche a quelle forme di criminalità non informatica. In tal modo, l'art. 23 individua l'ambito generale dell'obbligo di cooperazione: essa va estesa a tutti i reati collegati ai sistemi informatici e dati informatici, nonché alla raccolta di prove in forma elettronica di un reato. L'operatività della cooperazione internazionale prevista dalla Convenzione di Budapest non si limita solo ai reati commessi mediante l'uso di un sistema informatico, ma si applica anche laddove un crimine ordinario non commesso mediante un sistema informatico (ad es. un omicidio, una rapina o un attentato terroristico) comporta prove elettroniche.

Tuttavia, in un'ottica sistematica, va considerato che sia l'art. 33 (mutua assistenza nella raccolta in tempo reale di dati sul traffico), sia l'art. 34 (mutua assistenza in materia di intercettazioni di dati relativi al contenuto) consentono agli Stati di prevedere un diverso ambito di applicazione di queste misure, limitando il livello di cooperazione.

Con il principio di conformità si conviene che la cooperazione debba essere svolta «in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale». Tale clausola stabilisce il principio generale secondo cui le disposizioni del capitolo III non sostituiscono le disposizioni degli accordi internazionali sulla mutua assistenza giudiziaria, sia generali sia particolari, o disposizioni di diritto interno relative alla cooperazione internazionale⁵⁸³, ma si aggiungono ad esse.

Se ai fini della formazione della prova elettronica non rileva la disciplina relativa all'estradizione (art. 24) – essendo una procedura *in personam* – di notevole impatto sono i principi generali stabiliti per la mutua assistenza. L'art. 25 individua i principi generali relativi alla mutua assistenza ed integra quanto stabilito dall'art. 23.

La norma⁵⁸⁴ esordisce ribadendo i tre principi alla base della cooperazione giudiziaria nella Convenzione di Budapest, rimarcando come questa si estenda anche alla formazione

⁵⁸¹ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 242, p. 42. Sul punto, P. CSONKA, *The Council of Europe Convention on Cyber-Crime: a response to the Challenge of the New Age?*, cit., p. 27.

⁵⁸² Così, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 704 ss.

⁵⁸³ Il principio è poi esplicitamente rafforzato negli artt. 24 (estradizione), 25 (principi generali relativi alla mutua assistenza), 26 (informazioni spontanee), 27 (procedure relative alle richieste di mutua assistenza in assenza di accordi internazionali applicabili), 28 (confidenzialità e limitazioni di utilizzo), 31 (mutua assistenza concernente l'accesso a dati informatici immagazzinati), 33 (mutua assistenza nella raccolta in tempo reale di dati sul traffico) e 34 (mutua assistenza in materia di intercettazione di dati relativi al contenuto).

⁵⁸⁴ Per un commento, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 714; M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 318; A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law*

di prove elettroniche il cui oggetto non sia necessariamente un reato relativo a sistemi o dati informatici, per rispondere alla necessità di ottenere meccanismi semplificati di cooperazione internazionale.

Gli Stati, inoltre, si impegnano a adottare le misure legislative che siano eventualmente necessarie per adempiere agli obblighi imposti dal sistema di cooperazione giudiziaria, così come strutturato dal capitolo III. L'obbligo di avere una base giuridica per attuare le forme specifiche di cooperazione descritte nel resto del Capitolo (se i loro trattati, leggi e accordi non contengono già tali disposizioni) è di vitale importanza per una cooperazione in materia penale che voglia essere largamente efficace, poiché consentirebbe di rendere operativi i meccanismi indicati agli artt. 29 ss.

È inoltre prevista una procedura d'urgenza che assicura una maggior rapidità, tentando di garantire sicurezza ed autenticazione delle comunicazioni e del dato informatico.

L'obiettivo del paragrafo 3 è quello di facilitare l'accelerazione del processo di ottenimento dell'assistenza reciproca in modo che le informazioni o le prove critiche non vadano perse perché sono state cancellate prima che una richiesta di assistenza potesse essere preparata, trasmessa e risposta⁵⁸⁵. Si risponde così al pericolo di dispersione della prova elettronica, caratterizzata da alta volatilità, ovvero si accelerano i tempi al fine di consentire l'acquisizione del dato prima della scadenza del termine in cui esso è eliminato dal *service provider*. Inoltre, può rispondere all'esigenza di evitare danni significativi a persone o cose nelle ipotesi in cui le prove non vengono raccolte con rapidità.

Gli Stati, inoltre, sono autorizzati a fare richieste urgenti di cooperazione attraverso mezzi di comunicazione accelerati, piuttosto che attraverso la trasmissione tradizionale e molto più lenta di documenti scritti e sigillati attraverso buste diplomatiche o sistemi di consegna della posta. Lo Stato richiesto, a sua volta, deve accettare la domanda e rispondere alla richiesta con uno qualsiasi dei mezzi rapidi di comunicazione che garantiscano sicurezza ed autenticazione, come può essere, ad esempio, una piattaforma comune online.

La norma indica quali strumenti rapidi di comunicazione il fax e la posta elettronica, tuttavia pare opportuno ritenere che sia un elenco meramente indicativo. Non è escluso, infatti, l'uso di qualsiasi altro mezzo di comunicazione accelerato, purché risponda ai principi di sicurezza e autenticazione.

Non è indicato, invece, il livello minimo di sicurezza e autenticità richiesto, per cui sembra che le Parti possano decidere di comune accordo le forme a garanzia dell'autenticità delle comunicazioni e stabilire, eventualmente, necessarie misure di sicurezza speciali, come la crittografia, indispensabili in casi particolarmente delicati.

Il sistema di semplificazione delle comunicazioni, se da un lato accelera la procedura, dall'altra apre a possibili riduzioni di garanzia. Per questo, si è correttamente proceduto ad un bilanciamento, tentando, nel rispetto del vincolo di proporzione, di attuare un meccanismo di compensazione che renda la procedura armonica con i diritti fondamentali.

A tale obiettivo sembra rispondere la previsione di strumenti che garantiscano sicurezza ed autenticazione, ma soprattutto l'eventuale ordine di conferma. Con quest'ultimo, lo Stato richiesto potrebbe (se lo desidera) esigere dallo Stato richiedente una ulteriore conferma formale, inviata attraverso i tradizionali canali di comunicazione.

Enforcement in Global Cybercrime Cases, cit., p. 15; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 511 ss.

⁵⁸⁵ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 256, p. 44.

Il paragrafo 4 opera un rinvio alle condizioni previste dalla legislazione della Parte richiesta (secondo lo schema della *lex loci*) o ai trattati di mutua assistenza applicabili, inclusi i motivi di rifiuto. Si stabilisce così il principio di assistenza reciproca soggetta ai vincoli dei trattati di mutua assistenza e alle leggi nazionali⁵⁸⁶.

La norma si riferisce sia alle condizioni sia ai motivi di rifiuto, previsti secondo principio di legalità, che possono essere eccepiti dallo Stato di esecuzione della rogatoria attraverso i quali è possibile rifiutare la cooperazione. Con il rifiuto, l'esecuzione della domanda di assistenza è negata e, di conseguenza, non è dato seguito alla richiesta.

In tal modo, si rafforzano le garanzie per i diritti delle persone che si trovano nel territorio della Parte richiesta e che possono diventare oggetto di una richiesta di assistenza reciproca; di converso, si abbate il grado di fiducia reciproca, in piena coerenza con il principio strutturale della mutua assistenza⁵⁸⁷.

Tuttavia, una clausola di salvezza posta in apertura di paragrafo esclude l'operatività della disposizione quando sia espressamente previsto dagli articoli che compongono il capitolo III⁵⁸⁸. Scopo della clausola è segnalare le diverse eccezioni significative al principio generale contenute dalla Convenzione⁵⁸⁹.

Una prima eccezione è prevista per i motivi di rifiuto nello stesso par. 4, sicché lo Stato richiesto non può rifiutare l'esecuzione dell'attività rogatoria per i reati previsti dalla Convenzione⁵⁹⁰ e recepiti dagli Stati parte per il solo motivo che la richiesta riguardi un reato che esso reputi di natura fiscale⁵⁹¹. Ulteriore eccezione è contenuta all'art. 29, par. 3, secondo cui per la conservazione di dati informatici non può essere apposto come motivo di rifiuto l'assenza di una doppia incriminazione, salvo quanto previsto dal paragrafo 4 dello stesso articolo.

Infine, il paragrafo 5 fornisce una definizione di doppia incriminazione, limitando al contempo la portata del principio. Qualora consentito dalla Convenzione, la Parte richiesta può esigere – quale condizione di procedibilità – la doppia incriminazione. Qualora manchi, può opporre l'assenza di essa quale motivo di rifiuto.

Va rimarcato che la doppia incriminazione non sembra assumere la forma di una regola, bensì di una eccezione, poiché la riserva di legge sembra limitarne l'utilizzo alle sole ipotesi previste dalla Convenzione⁵⁹².

La condizione di procedibilità si considera soddisfatta, se la condotta alla base del reato per il quale si procede è anche un reato ai sensi delle leggi della Parte richiesta, anche se tali leggi collocano il reato in una diversa categoria di reato o usi una terminologia diversa nella denominazione del reato. In tal modo si evita il pericolo di adozione discrezionale di un criterio rigido di doppia incriminazione da parte degli Stati

⁵⁸⁶ Cfr., L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, cit., p. 1209.

⁵⁸⁷ Ad esempio, una misura intrusiva, come la perquisizione e il sequestro, non viene eseguita per conto di una Parte richiedente, a meno che non siano stati soddisfatti i requisiti fondamentali della Parte richiesta per tale misura applicabile in un caso nazionale. Le Parti possono anche garantire la protezione dei diritti delle persone in relazione agli oggetti sequestrati e forniti attraverso l'assistenza giudiziaria reciproca.

⁵⁸⁸ Il riferimento è all'inciso: «Salva contraria disposizione espressamente prevista negli articoli del presente capitolo».

⁵⁸⁹ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 258, p. 45.

⁵⁹⁰ Si tratta dei reati previsti dall'art. 2 all'art. 11.

⁵⁹¹ La disposizione a suo tempo è stata vigorosamente contrastata dalla delegazione svizzera, ma è stata comunque formulata. Sulla disposizione, inoltre, non è ammissibile riserva, così come stabilito all'art. 42. Sul punto, C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cybercriminalità*, cit., p. 512.

⁵⁹² Ad esempio, se una Parte richiesta si è riservata il diritto di richiedere la doppia incriminazione per quanto riguarda la conservazione dei dati ai sensi dell'art. 29, par. 4.

e si individua un criterio ermeneutico per valutare la sussistenza della condizione in caso di dubbi che, all'evidenza, possono sorgere nelle variazioni della terminologia e della categorizzazione della condotta criminale tra sistemi giuridici nazionali differenti⁵⁹³.

Uno Stato può anche trasmettere discrezionalmente ad un'altra Parte informazioni ottenute nel corso di proprie indagini. Si tratta di informazioni spontanee trasferibili alle autorità giudiziarie di un altro ordinamento nazionale che sembrano assumere le forme della "cortesia istituzionale", perché lo Stato di trasmissione ne ha facoltà, ma non l'obbligo.

Ai sensi dell'art. 26, l'invio delle informazioni deve avvenire nei limiti della propria legislazione nazionale e non è prevista quale presupposto una richiesta preventiva da parte dello Stato ricevente.

La trasmissione spontanea delle informazioni può avvenire qualora lo Stato ritenga che la comunicazione di esse possa aiutare lo Stato di recezione sia nell'avvio che nello svolgimento di indagini o processi che riguardino i reati così come definiti dalla Convenzione⁵⁹⁴.

Il limite ai reati contenuti nella Convenzione non opera in caso di informazioni connesse a richieste inviate da uno Stato ai sensi della Convenzione. In tal caso, lo Stato di trasmissione può inviare informazioni spontanee anche per fattispecie di reato non descritte nella Convenzione di Budapest, purché siano ricollegabili ad una richiesta inviata in base alla Convenzione, anche avente ad oggetto un reato comune o non previsto dalla stessa.

La trasmissione spontanea di informazioni presuppone un alto grado di collaborazione tra istituzioni ed un elevato livello di fiducia reciproca tra Stati. Pertanto, la norma si limita a delle previsioni di principio e sembra che lasci in capo agli Stati un'ampia discrezionalità.

Ratio della norma è consentire ad uno Stato in possesso di preziose informazioni, per le indagini o per i processi penali di un altro Stato di cui la Parte interessata non sia a conoscenza, di contribuire alla collezione di informazioni inerenti a un procedimento instauratosi in un altro ordinamento nazionale, utili per il contrasto alla criminalità. Inoltre, la divulgazione spontanea di informazioni non sembra precludere la possibilità allo Stato di trasmissione, se avente giurisdizione, di avviare indagini o processi in relazione ai fatti divulgati.

L'art. 26 non è un *novum* nel settore dell'assistenza giudiziaria⁵⁹⁵. Invero, l'articolo deriva da disposizioni di precedenti strumenti previsti dal Consiglio d'Europa, come l'art. 10 della Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di

⁵⁹³ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 258, p. 45.

⁵⁹⁴ In tal senso, M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 318; C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 512.

⁵⁹⁵ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 260, p. 46.

reato del 1990⁵⁹⁶ e l'art. 28 della Convenzione penale sulla corruzione⁵⁹⁷. Analoga previsione è prevista anche all'art. 20 della Convenzione sul riciclaggio, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo del 2005⁵⁹⁸. Il quadro si

⁵⁹⁶ La Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato (STE n. 141) è stata firmata a Strasburgo e aperta alla firma degli Stati membri e degli Stati non membri i quali hanno partecipato alla sua elaborazione e all'adesione degli altri Stati non membri l'8 novembre 1990. È entrata in vigore il 1° settembre 1993 ed al 4 gennaio 2021 è stata ratificata da 49 Stati. In Italia la Convenzione è stata ratificata con l. 9 agosto 1993, n. 3285, in GU 28 agosto 1993, n. 202, ed è entrata in vigore il 1° maggio 1994. Lo scopo della Convenzione è facilitare la cooperazione internazionale e l'assistenza per le indagini, la ricerca, il sequestro e la confisca dei proventi di ogni tipo di reato. La Convenzione tende ad aiutare le Parti a raggiungere simili livelli di efficacia, anche in assenza di una legislazione completa. In particolare, le Parti si impegnano: a prevedere fattispecie di reato per il riciclaggio dei proventi di reato; a confiscare gli strumenti ed i proventi (o dei beni il cui valore corrisponde a tali proventi). Ai fini della cooperazione internazionale, la Convenzione prevede: forme di assistenza investigativa (aiuto nella raccolta di elementi di prova, trasmissione ad altro Stato di informazioni, anche senza richiesta, adozione di tecniche investigative comuni, eliminazione del segreto bancario); misure provvisorie (congelamento di conti bancari, sequestri di beni per impedire la loro fuga); misure di confische dei proventi di reato (esecuzione da parte dello Stato richiesto di una decisione di confisca resa all'estero, apertura da parte dello Stato richiesto su domanda di un altro Stato di una procedura di confisca).

⁵⁹⁷ La Convenzione penale sulla corruzione (STE n. 173) è stata firmata a Strasburgo e aperta alla firma degli Stati membri e degli Stati non membri i quali hanno partecipato alla sua elaborazione e all'adesione degli altri Stati non membri e dell'Unione europea il 27 gennaio 1999. È entrata in vigore il 1° luglio 2002 ed al 17 febbraio 2022 è stata ratificata da 48 Stati, tra cui anche la Bielorussia, Stato non membro del Consiglio d'Europa, che vi ha aderito. L'Italia ha ratificato la Convenzione con l. 28 giugno 2012, n. 110, in GU 26 luglio 2012, n. 173 ed è entrata in vigore il 1° ottobre 2013. La Convenzione è uno strumento ambizioso teso a coordinare la penalizzazione di un gran numero di pratiche espressione di fenomeni di corruzione. Prevede inoltre ulteriori misure nel campo del diritto penale e una migliore cooperazione internazionale per perseguire i reati di corruzione. La sua applicazione è controllata dal "Gruppo di Stati contro la Corruzione – GRECO". La portata della Convenzione è molto vasta e completa gli strumenti giuridici esistenti. Copre le seguenti forme di condotta considerate normalmente come tipi specifici di corruzione: corruzione attiva e passiva di pubblici ufficiali nazionali e stranieri; corruzione attiva e passiva di parlamentari nazionali e stranieri e di membri di assemblee parlamentari internazionali; corruzione attiva e passiva nel settore privato; corruzione attiva e passiva di funzionari internazionali; corruzione attiva e passiva di giudici nazionali, stranieri ed internazionali e di funzionari di tribunali internazionali; traffico di influenze attivo e passivo; riciclaggio dei proventi della corruzione; reati contabili (fatture, falso in documenti contabili, ecc.) connessi con reati di corruzione. Gli Stati devono prevedere sanzioni e misure efficaci e dissuasive, ivi compresa la privazione della libertà, fino all'estradizione. Le persone giuridiche saranno anch'esse penalmente responsabili per i reati commessi per avvantaggiarle e potranno essere loro inflitte efficaci sanzioni penali o civili, comprese delle sanzioni pecuniarie. La Convenzione comprende inoltre delle disposizioni relative al concorso in corruzione e alla complicità, all'immunità, ai criteri per determinare la giurisdizione degli Stati, alla responsabilità delle persone giuridiche, all'istituzione di enti specializzati contro la corruzione, alla protezione di quanti collaborano con le autorità incaricate delle indagini e dei procedimenti giudiziari, alla raccolta di prove e alla confisca dei proventi. Prevede un'accresciuta cooperazione internazionale (mutua assistenza, estradizione e scambio di informazioni) ai fini delle indagini e dell'incriminazione per i reati di corruzione.

⁵⁹⁸ La Convenzione sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo (STE n. 198) è stata firmata a Varsavia e aperta alla firma degli Stati membri, degli Stati non membri i quali hanno partecipato alla sua elaborazione e dell'Unione europea e all'adesione degli altri Stati non membri il 16 maggio 2005. È entrata in vigore il 1° maggio 2008 ed al 4 gennaio 2021 è stata ratificata da 37 Stati. L'Italia ha ratificato la Convenzione con l. 28 luglio 2016, n. 153, in GU 9 agosto 2016, n. 31 ed è entrata in vigore il 26 agosto 2016. Con essa, il Consiglio d'Europa ha deciso di aggiornare e ampliare la sua convenzione del 1990 per poter mettere in conto non soltanto il finanziamento del terrorismo attraverso il riciclaggio di denaro, ma anche attraverso attività lecite. Questa nuova convenzione rappresenta il primo strumento internazionale per la prevenzione e il controllo del riciclaggio di denaro e del finanziamento del terrorismo. Il testo mette in evidenza come il veloce accesso alle informazioni relative ai finanziamenti o alle risorse delle organizzazioni criminali, compresi i gruppi

completa con la disposizione di cui all'art. 729-bis c.p.p.⁵⁹⁹ Simile meccanismo – che apre ad una collaborazione quanto più vasta possibile – è così importante per le attività collaborative di stampo transfrontaliero, tanto da essere stata prevista analogamente anche all'art. 7 della Convenzione di mutua assistenza dell'Unione europea del 2000 nonché dalla Convenzione delle Nazioni Unite sul crimine organizzato.

Prima della trasmissione delle informazioni, in alcune circostanze, la Parte trasmittente potrebbe subordinare l'invio di queste ad una “condizione di riservatezza” o a una “condizione di limitazione d'uso”, chiedendo alla Parte ricevente che le informazioni siano mantenute riservate o usate solo in determinati casi.

In particolare, la riservatezza sarà considerata importante nei casi in cui possono essere messi in pericolo rilevanti interessi dello Stato che li fornisce qualora le informazioni siano rese pubbliche. Si tratta, ad esempio, di situazioni in cui è necessario proteggere l'identità di una fonte di prova o le caratteristiche di un mezzo di ricerca delle informazioni o il fatto che si sta indagando su un gruppo criminale⁶⁰⁰.

A seguito di tale richiesta, potrebbe essere necessaria l'instaurazione di un confronto dialettico tra le parti, qualora lo Stato ricevente non possa adeguarsi alla richiesta. Successivamente a queste comunicazioni, spetterà allo Stato di trasmissione stabilire se le informazioni debbano comunque essere trasmesse, nonostante non sia possibile mantenerne la riservatezza o non possano essere utilizzate alle condizioni richieste. Qualora la Parte ricevente accetti le informazioni alle condizioni stabilite, dovrà attenersi.

I principi generali sinora esposti rappresentano l'egida sotto cui si colloca l'intera disciplina relativa alla mutua assistenza giudiziaria per la formazione dell'*e-evidence*. L'art. 23 sancisce la base su cui si regge l'intera ossatura normativa relativa alla cooperazione giudiziaria di contrasto alla criminalità informatica e, più in generale, per la formazione della prova elettronica.

L'art. 25 si limita a prevedere una disciplina generale integrativa delle altre convenzioni o di accordi di mutua assistenza conclusi sulla base di una legislazione uniforme in vigore o in condizione di reciprocità, tant'è che non è né sussidiaria né alternativa a quanto stabilito da altre fonti, ma anzi assume una funzione di completamento di esse; diverso approccio dovrà aversi con quanto stabilito dall'art. 27.

Invero, gli Stati firmatari erano consapevoli delle evidenti carenze nel sistema convenzionale internazionale, per cui hanno previsto un meccanismo di cooperazione da attivare per la lotta alla criminalità informatica o per la formazione della prova elettronica ogniqualvolta mancasse una disciplina di riferimento o quando questa, pur esistendo, risultasse inefficace o poco pratica.

Di conseguenza, l'art. 27 rafforza il principio generale secondo cui l'assistenza reciproca dovrebbe essere effettuata mediante l'applicazione dei trattati pertinenti e di accordi per l'assistenza reciproca. Con tale Convenzione, i redattori hanno rifiutato l'idea di un regime generale di mutua assistenza separato ed autonomo, applicabile al posto di altri strumenti e disposizioni già previsti altrove. Hanno convenuto, invece, che sarebbe stato più pratico fare affidamento sui sistemi di mutua assistenza già operativi come

terroristici, è fondamentale per il successo delle misure preventive e repressive e, in ultima analisi, rappresenta il modo migliore per destabilizzare le attività di queste organizzazioni.

⁵⁹⁹ Per un commento sul sistema della trasmissione spontanea di informazioni, E. CALVANESE, *Cooperazione giudiziaria tra Stati e trasmissione spontanea di informazioni: condizioni e limiti di utilizzabilità*, in *Cass. pen.*, 2, 2003, p. 458 ss.

⁶⁰⁰ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 261, p. 46.

cornice generale, consentendo in tal modo agli operatori della mutua assistenza di utilizzare gli strumenti e le disposizioni con cui hanno maggiore familiarità ed evitare la confusione che potrebbe derivare dall'istituzione di regimi concorrenti.

Infine, solo per quanto riguarda particolari meccanismi necessari per una cooperazione rapida ed efficace in materia penale relativa alla criminalità informatica, come quelli di cui agli articoli da 29 a 35, ciascuna Parte è tenuta a stabilire una base giuridica per consentire lo svolgimento di tali forme di cooperazione, qualora non già previste dai suoi attuali trattati, accordi o leggi di mutua assistenza. Per cui, la maggior parte delle forme di mutua assistenza ai sensi della Convenzione continuerà ad essere attuata secondo gli strumenti che sono già o che saranno previsti da altre Convenzioni di mutua assistenza⁶⁰¹.

Ne è derivata una disciplina basata su un doppio binario: da una parte un compendio normativo rivolto a completare quanto già esistente nell'ambito della cooperazione di tipo rogatorio, dall'altra una disciplina "di chiusura", di sostegno agli Stati che non abbiano concluso accordi o trattati aventi ad oggetto le rogatorie o che, pur avendoli conclusi, ritengano maggiormente efficace la disciplina derivata in tutto o in parte dall'art. 27.

3. La mutua assistenza per la formazione dell'*e-evidence* prevista dalla Convenzione sulla criminalità informatica in assenza di accordi internazionali applicabili

L'interprete che si imbatte nella rubrica dell'art. 27⁶⁰² nota immediatamente una netta difformità tra quanto in essa indicato e quanto effettivamente disciplinato. Tale forte assunto si basa sulla consapevolezza che, a differenza della rubrica che pretende di prevedere una procedura relativa unicamente alle richieste di mutua assistenza in assenza di accordi internazionali applicabili, il contenuto dell'articolo disciplina anche l'applicazione della procedura "per accordo di parti".

Invero, la procedura rivela una duplice funzione alternativa: sussidiaria, poiché si applicano le disposizioni ivi previste, qualora non vi sia un trattato o un accordo di mutua assistenza concluso sulla base di una legislazione uniforme in vigore o in condizione di reciprocità tra la Parte richiedente e la Parte richiesta; surrogatoria, ovvero sostitutiva e

⁶⁰¹ In particolare, le rogatorie saranno attuate ai sensi della Convenzione europea di assistenza giudiziaria in materia penale (STE n. 30) e del suo protocollo (STE n. 99) tra le Parti di tali strumenti. In alternativa, le parti della presente Convenzione che hanno tra loro convenzioni bilaterali o altri accordi multilaterali che disciplinano l'assistenza reciproca in materia penale (come tra gli Stati membri dell'Unione europea, per i quali si applica la Convenzione MAP, ossia di mutua assistenza del 2000), continueranno ad applicare questi sistemi di riferimento, integrati da quanto stabilito dalle norme del Capitolo III della Convenzione sulla criminalità informatica, a meno che non acconsentano ad applicare una o tutte le disposizioni dell'art. 27 al posto di esse. L'assistenza reciproca può anche essere basata su accordi concordati sulla base di una legislazione uniforme o reciproca, come il sistema di cooperazione sviluppato tra i paesi nordici, che è ammesso anche dalla Convenzione europea di assistenza giudiziaria in materia penale (articolo 25, paragrafo 4), e tra i membri del *Commonwealth*. Infine, il riferimento a trattati o accordi di mutua assistenza sulla base di una legislazione uniforme o in condizione di reciprocità non si limita a quegli strumenti in vigore al momento dell'entrata in vigore della Convenzione di Budapest, ma copre anche gli strumenti che possono essere adottati in futuro.

⁶⁰² Cfr., J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 715 ss.; M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 318 ss.

supplementare, poiché si prevede che le parti possano accordarsi per applicare in tutto o in parte le regole dell'art. 27 al posto di un trattato, un accordo o una legislazione vigente.

Per cui, se da un lato vi è l'obbligo per gli Stati di applicare determinate procedure e condizioni di mutua assistenza qualora non vi siano trattati o accordi sulla base di una legislazione uniforme o condizione di reciprocità in vigore tra la Parte richiedente e la Parte richiesta; dall'altra si permette di applicare in tutto o in parte le disposizioni dei paragrafi da 2 a 9, in caso di intesa tra le Parti. È, del resto, evidente che sia stato demandato agli Stati interessati l'individuazione delle specifiche circostanze o clausole da applicare al caso concreto, nell'ipotesi in cui essi abbiano deciso di optare per un'applicazione parziale in funzione surrogatoria della disciplina di cui all'art. 27.

Una simile previsione sembra essere il frutto di riflessioni compiute sulla natura della prova digitale, caratterizzata per l'universalità, l'immaterialità, la dispersione, la promiscuità, la modificabilità, la volatilità, l'attitudine ad essere copiata all'infinito. Tali caratteristiche incidono sulle modalità di formazione, e di conseguenza, sul sistema di mutua assistenza più adatto.

Del resto, le peculiarità della prova elettronica consentono di prevedere modalità di formazione mediante rogatoria identiche a quelle utilizzate per le altre prove, procedendo tramite ispezioni, perquisizioni e sequestri informatici, ma adottando espedienti tecnici indispensabili affinché si assicuri la genuinità e la conservazione⁶⁰³.

Nel descrivere la procedura di formazione della prova informatica transnazionale, la norma fornisce una serie di regole, tra cui l'istituzione delle autorità centrali, l'imposizione di condizioni, motivi e procedure in caso di rinvio o rifiuto, riservatezza delle richieste e comunicazioni dirette.

Per quanto riguarda tali questioni espressamente trattate, in assenza di un trattato o di un accordo di mutua assistenza sulla base di una legislazione uniforme o condizione di reciprocità, le disposizioni devono essere applicate al posto delle leggi nazionali che disciplinano l'assistenza reciproca⁶⁰⁴. Allo stesso tempo, l'art. 27 non prevede regole per altre questioni normalmente trattate nella legislazione nazionale che disciplina l'assistenza reciproca internazionale. Ad esempio, non ci sono disposizioni riguardanti la forma e il contenuto delle richieste, l'assunzione di testimonianze delle Parti richieste o richiedenti, la fornitura di documenti ufficiali o aziendali, il trasferimento di testimoni in custodia o l'assistenza in materia di confisca. Riguardo a tali questioni, l'art. 25, par. 4, prevede che, in assenza di una disposizione specifica nel presente Capo, la legge della Parte richiesta disciplina le modalità specifiche per fornire quel tipo di assistenza⁶⁰⁵.

Innanzitutto, il paragrafo 2 chiede ad ogni Stato parte di designare una o più autorità centrali⁶⁰⁶. Queste sono organi di comunicazione che assumono anche funzioni amministrative, sono responsabili dell'invio o della risposta alle richieste di assistenza, eseguono le richieste e ne curano la trasmissione alle autorità nazionali legittimate.

La trasmissione diretta tra tali autorità è più rapida ed efficiente rispetto a quanto previsto dalle convenzioni che disciplinano i tradizionali sistemi di assistenza giudiziaria. Inoltre, l'istituzione di un'autorità centrale "attiva" assume un ruolo importante nel

⁶⁰³ In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 162 ss.

⁶⁰⁴ Le norme nazionali risultano sempre residuali e sussidiarie anche rispetto alle regole stabilite dalla Convenzione del Consiglio d'Europa sulla criminalità informatica.

⁶⁰⁵ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 264, p. 47.

⁶⁰⁶ L'art. 27, par. 2, lett. a) recita: «Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution».

garantire che le richieste in entrata e in uscita siano perseguite con diligenza e che venga fornita consulenza alle forze dell'ordine straniere su come soddisfare al meglio le richieste, in particolare quelle urgenti o delicate da trattare con adeguatezza⁶⁰⁷.

Il Consiglio d'Europa ha incoraggiato gli Stati a designare un'unica autorità centrale, per ragioni di efficienza. Si evita, così, una parcellizzazione di istituzioni che renda particolarmente complessa la cooperazione. Tuttavia, una Parte ha la possibilità di designare più di un'autorità centrale ove sia preferibile nell'ambito del proprio sistema di assistenza reciproca.

Qualora sia istituita più di un'autorità centrale, lo Stato dovrebbe garantire che tra autorità vi sia l'uniforme interpretazione delle disposizioni della Convenzione e che sia le richieste in entrata che quelle in uscita siano trattate rapidamente ed efficacemente.

Ciascuna Parte, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, è tenuta a comunicare al Segretariato Generale del Consiglio d'Europa i nomi e gli indirizzi (e-mail e fax) dell'autorità o delle autorità designate per ricevere e rispondere alle richieste di assistenza reciproca ed a indicare tempestivamente ogni sostituzione, al fine di garantire il tempestivo aggiornamento del registro delle autorità centrali ad opera del Segretariato del Consiglio d'Europa⁶⁰⁸.

La corretta pubblicità ed il rapido aggiornamento del registro delle autorità centrali consentono ai singoli Stati di individuare con celerità l'autorità centrale con cui comunicare per la formazione della prova elettronica. Ciò dovrebbe garantire la sollecita esecuzione delle operazioni poiché i canali di dialogo garantirebbero una maggiore speditezza rispetto a quanto stabilito in altre convenzioni di mutua assistenza, anche grazie al diretto collegamento tra autorità.

⁶⁰⁷ Cfr. *Explanatory Report to the Convention on Cybercrime*, par. 265, p. 47. Sul punto, anche, M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 318.

⁶⁰⁸ L'Italia ha designato un'unica autorità centrale con la Dichiarazione contenuta in due note verbali depositate con lo strumento di ratifica in data 5 giugno 2008. Ai sensi dell'art. 27, par. 2, della Convenzione, la Repubblica italiana ha dichiarato che dal 1° ottobre 2008 è designato quale autorità competente il Ministro della giustizia della Repubblica italiana. In Spagna, è stata designata quale autorità centrale la Sub-direzione generale per la cooperazione giuridica internazionale del Ministero della giustizia con la Dichiarazione contenuta nello strumento di ratifica depositata il 3 giugno 2010, con efficacia a partire dal 1° ottobre 2010. Differentemente, con la Dichiarazione contenuta nello strumento di ratifica depositato il 25 maggio 2011, la Gran Bretagna, ad esempio, ha scelto di indicare più autorità centrali. In particolare, sono state designate quali autorità centrali, con efficacia dal 1° settembre 2011, la UK Central Authority per questioni relative a Inghilterra, Galles e Irlanda del Nord; l'International Co-operation Unit per questioni relative alla Scozia; la Law Enforcement & International Advisory Division limitatamente alle questioni relative alla fiscalità indiretta. Scelta analoga a quella inglese si potrebbe prevedere per quelle Parti che hanno adottato una forma di Stato federale. Ebbene, la Germania ha invece optato per la designazione di un'unica autorità centrale con la dichiarazione contenuta in una lettera del Rappresentante permanente della Germania, in data 14 maggio 2009, registrata presso il Segretariato generale il 15 maggio 2009. A partire dal 1° luglio 2009, l'autorità centrale per la Germania è il Ministero degli Affari Esteri. Anche altri Stati federali quali il Belgio e l'Austria hanno optato per la designazione di un'unica autorità centrale, rispettivamente il Service Public Fédéral Justice – Service de la coopération internationale pénale con efficacia dal 1° dicembre 2012 e il Bundesministerium für Justiz – Abt. IV 4 Internationale Strafsachen con efficacia dal 1° ottobre 2012. Volgendo lo sguardo ai Paesi extra-europei, l'Australia ha designato quale autorità centrale l'International Crime Cooperation Central Authority Attorney-General's Department (periodo di efficacia dal 1° marzo 2013); l'Argentina ha designato il Directorate for International Mutual Legal Assistance of the Ministry of Foreign Affairs and Worship of the Argentine Republic (periodo di efficacia a partire dal 1° ottobre 2018); il Canada ha designato l'International Assistance Group of the Department of Justice (periodo di efficacia dal 7 novembre 2015); gli Stati Uniti d'America hanno designato l'Office of International Affairs, United States Department of Justice, Criminal Division, Washington.

L'istituzione di autorità centrali è particolarmente utile per garantire una reazione rapida, fondamentale nella lotta alla criminalità informatica o per la formazione della prova elettronica. Con esse, si evita che la trasmissione avvenga attraverso i tradizionali canali diplomatici, che rischierebbero di irrigidire e rallentare la procedura.

Tuttavia, il sistema non gode della stessa celerità prevista dagli strumenti di mutuo riconoscimento – come l'ordine europeo di indagine penale – che elidono totalmente il meccanismo previsto dal metodo intergovernativo, mettendo in diretto collegamento le autorità giudiziarie, e non politico-amministrative degli Stati coinvolti, con conseguente importante risparmio dei tempi per le indagini.

3.1. *La procedura*

La procedura di mutua assistenza è descritta nei dettagli dall'art. 27, par. 3 della Convenzione. Come per le altre procedure rogatorie, è suddivisibile in quattro fasi: emissione della richiesta di formazione della prova; verifica dell'assenza di motivi di rifiuto; esecuzione; utilizzabilità della prova elettronica nello Stato richiedente.

La richiesta va inoltrata dall'autorità centrale dello Stato richiedente all'autorità centrale dello Stato richiesto avendo cura di indirizzarla al recapito indicato nel registro delle autorità centrali⁶⁰⁹. Nulla si chiarisce relativamente alla lingua in cui vanno formulate le richieste, né sul contenuto di esse.

La richiesta potrebbe essere subordinata ad una clausola di riservatezza. In tale ipotesi, ai sensi dell'art. 27, par. 8, lo Stato richiedente potrebbe domandare alla Parte richiesta di mantenere «confidenziale il fatto e anche l'oggetto» della richiesta, eccetto, all'evidenza, nella misura in cui sia necessario per la sua esecuzione. Si tratta di circostanze relative a casi particolarmente delicati o in cui una *discovery* prematura potrebbe condurre a conseguenze negative.

Tuttavia, per evidenti ragioni ontologiche, pare che non sia possibile reclamare la riservatezza ogniqualvolta rischi di compromettere la capacità dello Stato di esecuzione di ottenere le prove o le informazioni ad oggetto⁶¹⁰. Quando non è possibile ottemperare alla richiesta di riservatezza, lo Stato richiesto informa lo Stato richiedente, il quale potrà ritirare o modificare la richiesta.

Nulla di più è stabilito in relazione ai poteri dell'autorità centrale, per cui bisogna far riferimento alla disciplina interna. Generalmente, è necessario che si superi un vaglio di ammissibilità basato su presupposti delineati dall'ordinamento dello Stato di emissione e che attengono all'*an* delle operazioni istruttorie, volti a verificare il rispetto dei diritti fondamentali. Ad esempio, nel caso di indagini informatiche, va constatato il rispetto del

⁶⁰⁹ Norma analoga è prevista nella Convenzione europea di assistenza giudiziaria in materia penale, la quale all'art. 15 stabilisce che «Le commissioni rogatorie previste negli articoli 3, 4 e 5 e le domande previste nell'articolo 11 saranno trasmesse dal Ministero di Giustizia della Parte richiedente al Ministero di Giustizia della Parte richiesta e rispedita per la stessa via». Orbene, mentre la Convenzione sulla criminalità informatica lascia in capo agli Stati un ampio margine di libertà nell'individuazione di una o più autorità centrali, la Convenzione di assistenza giudiziaria del 1959, più rigida nell'applicazione del principio di mutua assistenza e del metodo intergovernativo, richiede espressamente che i canali di comunicazioni per le richieste siano tra Ministeri della giustizia.

⁶¹⁰ Si tratta di ipotesi in cui le informazioni devono essere divulgate per ottenere l'autorizzazione di un tribunale per fornire assistenza, oppure i casi in cui vi siano persone (anche giuridiche) in possesso di elementi di prova che dovranno inevitabilmente conoscere la richiesta affinché possa essere eseguita con successo la richiesta. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 273, p. 49.

diritto alla riservatezza previsto dagli art. 14 e 15 Cost., 8 CEDU e 7 e 8 della Carta dei diritti fondamentali dell'UE, poiché si tratterebbe di attività intrusive di luoghi virtuali, ricchi di informazioni relative alla vita privata delle persone⁶¹¹.

La disciplina relativa a richieste di assistenza inviate dall'Italia appare farraginosa, il che favorisce la dispersione dell'elemento probatorio informatico o comunque contribuisce alla difficile formazione. Ed invero, in applicazione di quanto stabilito dalla disciplina sussidiaria di cui all'art. 727 c.p.p., l'autorità giudiziaria che intende richiedere un'attività di natura investigativa e/o che abbia attitudine probatoria deve ricorrere al metodo intergovernativo, con conseguente attivazione del filtro politico del Ministro della giustizia⁶¹², il quale «può disporre con decreto che non si dia corso all'inoltro della richiesta di assistenza giudiziaria nei casi e nei limiti stabiliti dalle convenzioni» ed in caso di pericolo per la sovranità, la sicurezza o altri interessi essenziali dello Stato⁶¹³.

Qualora la richiesta di assistenza non sia stata inoltrata entro trenta giorni dalla ricezione e non sia stato emesso il decreto, l'autorità giudiziaria potrà usufruire dei canali diplomatici previsti dal comma 4, inoltrando direttamente la richiesta all'agente diplomatico o consolare italiano, ed informandone il Ministro. In capo al Ministro sono inoltre previsti oneri di carattere amministrativo, dovendo egli procedere alla trasmissione delle richieste di assistenza giudiziaria per «comunicazioni, notificazioni e per attività di acquisizione probatoria»⁶¹⁴. Proprio la comunicazione “indiretta” tra autorità giudiziarie – filtrata dai canali istituzionali ministeriali – rappresenta uno degli elementi di maggiore lentezza delle procedure, con conseguente danno per la formazione dell'*e-evidence*⁶¹⁵.

⁶¹¹ In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1623.

⁶¹² Come efficacemente osservato dalla dottrina, «i poteri di blocco spettanti al Ministro si riconducono a valutazioni di opportunità politica o di ammissibilità giuridica *ictu oculi* della richiesta». Cfr., G. DI CHIARA, *Rapporti giurisdizionali con autorità straniere*, in *Enc. giur.*, Agg. II, Milano, 1998, p. 891.

⁶¹³ La giurisprudenza ha inoltre chiarito che gli atti compiuti all'estero su rogatoria sono assunti generalmente seguendo la *lex loci*, salvo il contrasto con norme inderogabili di ordine pubblico e buon costume, «che non debbono necessariamente identificarsi con il complesso delle regole dettate dal codice di rito ed in particolare con quelle relative all'esercizio dei diritti della difesa». Cass., Sez. I, sentenza del 5 dicembre 2002, n. 41005, in *Ced Cass.*, rv. 223202. V., inoltre, Cass., Sez. VI, sentenza del 18 novembre 2004, n. 44830, in *Ced Cass.*, rv. 230594; Cass., Sez. I, sentenza del 25 gennaio 2008, n. 4060, in *Ced Cass.*, rv. 239193. Più di recente, la giurisprudenza non ha parlato più di ordine pubblico e buon costume, bensì di «norme inderogabili e principi fondamentali». In tal senso, Cass., Sez. V, sentenza del 23 ottobre 2007, n. 39020, in *Ced Cass.*, rv. 238207; Cass., Sez. I, sentenza del 26 maggio 2009, n. 21673, in *Ced Cass.*, rv. 243795.

⁶¹⁴ L'art. 727, comma 1, c.p.p. usa il termine polivalente di “acquisizione” probabilmente al fine di includere nelle attività di carattere probatorio sia quelle relative a prove pre-formate, sia quelle relative ad una formazione della prova che si otterrà attraverso un mezzo di prova nel processo. Invero, in dottrina, si tende ad usare il termine “acquisizione” con riguardo alle prove pre-costituite, mentre il termine “assunzione” sarebbe riferibile ai mezzi di prova che si costruiscono nel processo. Tuttavia, come acutamente osservato, il termine “acquisizione” è usato anche in altri significati. Infatti, «è possibile prospettare una pluralità di ipotesi in base alle quali il riferimento all'acquisizione viene utilizzato, ora, come un vero e proprio sinonimo di assunzione, ora, come un meccanismo di assunzione indiretta mediante il ricorso alle letture dibattimentali. Il quadro è tutt'altro da ritenersi esaurito, in quanto tra le prospettive da sottoporre al banco di prova rientrano anche quelle volte ad assegnare all'acquisizione sia il significato di meccanismo di ingresso nel dibattimento di quei mezzi di prova, per natura, precostituiti, sia il significato di fenomeno generale diretto a consentire la formazione del sapere in vista del giudizio». Cfr., L. KALB, *Il documento nel sistema probatorio*, cit., p. 216.

⁶¹⁵ Il procedimento risulta comunque più veloce rispetto alla disciplina previgente al d. lgs. 3 ottobre 2017, n. 149. Invero, si disponeva che l'inoltro delle richieste non avvenisse direttamente all'autorità estera, bensì era richiesto di avvalersi dei canali diplomatici. Per un approfondimento sulla rogatoria “attiva”, A. ANZON, *Interpretazione “corretta” e interpretazione “conforme a Costituzione” del regime delle rogatorie*

Ugualmente lenta è la procedura di rogatoria dall'estero. I poteri dell'autorità centrale sono descritti all'art. 723 c.p.p., secondo cui il Ministro della giustizia può non dar corso all'esecuzione della richiesta di assistenza giudiziaria non solo nei casi e nei limiti stabiliti dalle convenzioni e dagli atti adottati dal Consiglio e dal Parlamento dell'Unione europea quando coinvolgono rapporti con Stati membri dell'Ue, ma anche in caso di pericolo per la sovranità, la sicurezza o altri interessi essenziali dello Stato, ovvero quando risulta evidente che gli atti richiesti sono espressamente vietati dalla legge o sono contrari ai principi fondamentali dell'ordinamento giuridico italiano o ancora quando vi siano fondate ragioni per ritenere che considerazioni relative alla razza, alla religione, al sesso, alla nazionalità, alla lingua, alle opinioni politiche o alle condizioni personali o sociali possano influire negativamente sullo svolgimento o sull'esito del processo e non risulta che l'imputato abbia liberamente espresso il suo consenso alla rogatoria, nelle ipotesi in cui siano in esame rapporti con Stati diversi da quelli membri dell'Unione europea⁶¹⁶.

internazionali, in *Giur. Cost.*, 4, 2002, p. 2426 ss.; A. ASTARITA, *Vecchio e nuovo in tema di rogatorie internazionali*, in *Giur. it.*, 1, 2003, p. 150 ss.; G. BARROCU, *Rogatorie penali internazionali*, in *Enc. dir.*, XXX, Roma, 2008, p. 1 ss.; D. CARCANO, *In tema di rogatorie internazionali*, in *Cass. pen.*, 11, 2002, p. 3333 ss.; G. CATELANI, *I rapporti internazionali in materia penale*, Milano, 1995, *passim*; M. CHIAVARIO, *Cooperazione internazionale ed obiettivi di garanzia e di efficienza nella nuova disciplina dei rapporti con autorità giudiziarie straniere*, in *Leg. Pen.*, 4, 1990, p. 687 ss.; G. DARAIO, *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), cit., p. 1120 ss.; ID., voce *Rogatorie internazionali*, in AA.VV., *Digesto del Processo penale* (diretto da A. SCALFATI), Torino, 2012, p. 1 ss.; ID., *Le rogatorie internazionali*, in AA.VV., *Trattato di procedura penale* (diretto da G. SPANGHER), vol. 6, *Esecuzione e rapporti con autorità giurisdizionali straniere* (a cura di L. KALB), Milanofiori Assago, 2009, p. 617 ss.; G. DE DONATO, *L'attività del ministro della giustizia in tema di rogatorie attive e passive*, in AA.VV., *Rogatorie penali e sviluppi della cooperazione giudiziaria internazionale* (a cura di G. LA GRECA, M.R. MARCHETTI), Torino, 2003, p. 383 ss.; A. DE FRANCESCO, *Inutilizzabili le rogatorie assunte all'estero in contrasto con le norme inderogabili di ordine pubblico e buon costume*, in *Dir e giust.*, 12 dicembre 2012, p. 1080 ss.; G. DI CHIARA, *Invio di documenti nella rogatoria internazionale*, in *Foro it.*, 10, 2002, p. 2564 ss.; G. DIOTALLEVI, sub *Art. 723*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 183 ss.; N. GALANTINI, *La cooperazione internazionale per la ricerca e l'acquisizione della prova*, in AA.VV., *Argomenti di procedura penale internazionale* (a cura di O. DOMINIONI), Milano, 1982, p. 39 ss.; M.R. MARCHETTI, *Rapporti giurisdizionali con autorità straniere*, in AA.VV., *Compendio di procedura penale* (a cura di G. CONSO, V. GREVI, M. BARGIS) Padova, 2014, p. 1161 ss.; ID., *Cooperazione giudiziaria: innovazioni apportate e occasioni perdute*, cit., p. 1545 ss.; F. NUZZO, *Indicazioni della Corte costituzionale in tema di rogatorie all'estero*, in *Cass. pen.*, 11, 2002, p. 3334 ss.; L. PRIMICERIO, *Riesaminabilità del decreto di sequestro eseguito per rogatoria all'estero*, in *Cass. pen.*, 10, 2003, p. 2996 ss.; M. SCAPARONE, *Procedura penale*, vol. II, Torino, 2008, p. 418 ss.; A. VENEGONI, *Rogatorie*, in *Cass. pen.*, 5, 2017, p. 393 ss.

⁶¹⁶ La norma è frutto della recente riforma che ha riordinato e riscritto la disciplina dell'assistenza rogatoria contenuta nel codice di procedura penale. Il legislatore ha optato per un contenimento dei poteri attribuiti all'autorità ministeriale, riordinandoli al fine di evitare sovrapposizioni. Attraverso l'ampia clausola prevista, al Ministro è conferito un forte potere di blocco, ritenuto dalla dottrina ineliminabile in ragione dell'«imprevedibile varietà delle circostanze e dei potenziali richiedenti assistenza». Sul punto, T. RAFARACI, *Rogatorie*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX convegno nazionale. Roma, 20-21 ottobre 2016* (a cura di L. KALB), Milano, 2017, p. 43. V., altresì, E. CESQUI, *Il ruolo del Ministero nella cooperazione penale*, in *Cass. pen.*, 1, 2019, p. 14 ss.; M.R. MARCHETTI, *Prospettive di riforma del libro XI c.p.p.*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX convegno nazionale. Roma, 20-21 ottobre 2016* (a cura di L. KALB), Milano, 2017, p. 27 ss. Sulla procedura di assistenza giudiziaria così come disciplinata attualmente nel c.p.p., *ex multis*, G. DI PAOLO, *La riforma della disciplina codicistica delle rogatorie internazionali (D.Lg. 3 ottobre 2017, n. 149)*, in *Cass. pen.*, 10, 2018, p. 3425 ss.; G. DIOTALLEVI, sub *Art. 723*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), cit., p. 155 ss.; M.R. MARCHETTI, *Cooperazione giudiziaria: innovazioni apportate e occasioni perdute*, cit., p. 1547 ss.; F. RUGGIERI, *Il libro XI del codice di rito. Guida minima*, in *Cass. pen.*, 5, 2018, p. 1766 ss.; ID., *La legge delega in tema di cooperazione penale internazionale: la montagna ha*

A questa fase, di carattere squisitamente politico-amministrativo, segue una fase giurisdizionale di tipo cognitivo, volta a verificare se sussistano presupposti su cui fondare il rifiuto dell'esecuzione.

La Convenzione sulla criminalità informatica nulla chiarisce sul legittimato a valutare l'esistenza dei motivi di rifiuto; pertanto, si ritiene che sia applicabile la disciplina nazionale sussidiaria prevista dai singoli ordinamenti nazionali. In Italia, ai sensi dell'art. 724 c.p.p., legittimato ai controlli di *exequatur* è il Procuratore della Repubblica presso il Tribunale del capoluogo del distretto del luogo nel quale deve compiersi l'attività richiesta⁶¹⁷, il quale, ricevuti gli atti trasmessi dal Ministro della giustizia, dovrà valutare l'ammissibilità della richiesta, opponendo eventuali motivi di rifiuto⁶¹⁸.

La dottrina ritiene che la scelta di legittimare l'ufficio del Pubblico ministero sia espressione di semplificazione e snellezza della procedura, manifestazione di una assistenza che individua il proprio fulcro nella matrice investigativa, e di conseguenza affida a tale autorità giudiziaria il compito di verificare l'ammissibilità delle richieste, in risposta ad evidenti esigenze di efficienza⁶¹⁹.

La Convenzione individua i motivi per cui è possibile rifiutare l'assistenza, secondo quanto stabilito dal principio strutturale della mutua assistenza, il quale, a differenza del mutuo riconoscimento, non postula l'esecuzione obbligatoria⁶²⁰. Oltre a quanto stabilito con la previsione dell'art. 25, par. 4, che estende il novero dei motivi di rifiuto a quelli previsti dalla legislazione della Parte richiama⁶²¹, l'art. 27, par. 4 indica tra gli altri motivi di rifiuto la richiesta relativa a reati politici o connessi e il pregiudizio per la propria sovranità, sicurezza, ordine pubblico o altri interessi essenziali⁶²².

partorito un topolino?, in *Proc. pen. e giust.*, 2, 2017, p. 315 ss.; E. SELVAGGI, *Quel "restyling" che facilita la ricerca di chi è latitante*, cit., p. 66 ss.; ID., *Va "in soffitta" l'atto di exequatur della Corte d'Appello*, in *Guida al diritto*, 45, 4 novembre 2017, p. 73 ss.; N. TRIGGIANI, *In divenire la disciplina dei rapporti con autorità straniera: appunti sulla l. 21 luglio 2016, n. 149*, in *penalecontemporaneo.it*, 5 ottobre 2016, disponibile al link:

https://archiviodypc.dirittopenaleuomo.org/upload/1473880246TRIGGIANI_2016b.pdf; G. UBERTIS, *Considerazioni generali su investigazioni e prove transnazionali*, in *Cass. pen.*, 1, 2017, p. 49B ss.

⁶¹⁷ Salvo che si tratti di atto del giudice o per il quale sia richiesta autorizzazione del giudice, nel qual caso quest'ultimo sarà chiamato in causa.

⁶¹⁸ Qualora l'autorità richiedente o l'ordinamento italiano postulino che l'atto istruttorio venga compiuto o autorizzato da un giudice, vi provvederà il giudice per le indagini preliminari.

⁶¹⁹ Sul punto, T. RAFARACI, *Rogatorie*, cit., p. 43. Altra dottrina ritiene, inoltre, che «affidare tale verifica al giudice fornisce di per sé una migliore garanzia, nondimeno, in nome dell'efficienza e della snellezza, il legislatore delegante ha ritenuto preferibile eliminarne l'intervento anche per evitare trasmissioni, sicuramente onerose in termini di tempo, dal giudice all'autorità competente per l'esecuzione costituita, nel caso delle indagini, proprio dal pubblico ministero al quale sono affidate nel procedimento interno». Cfr. M.R. MARCHETTI, *Prospettive di riforma del libro XI c.p.p.*, cit., p. 28.

⁶²⁰ Cfr., quanto previsto in generale dall'art. 696-bis c.p.p., tuttavia attenuato dall'esigenza di proteggere i diritti fondamentali, così come indicato dall'art. 696-ter c.p.p.

⁶²¹ Per lo Stato italiano, questi sono contenuti nell'art. 724, comma 7, c.p.p., secondo il quale «L'esecuzione della domanda di assistenza è negata: a) se gli atti richiesti sono vietati dalla legge o sono contrari ai principi dell'ordinamento giuridico dello Stato; b) se il fatto per cui procede l'autorità straniera non è previsto come reato dalla legge italiana e non risulta che l'imputato abbia liberamente espresso il suo consenso alla domanda di assistenza giudiziaria; c) se vi sono fondate ragioni per ritenere che considerazioni relative alla razza, alla religione, al sesso, alla nazionalità, alla lingua, alle opinioni politiche o alle condizioni personali o sociali possano influire sullo svolgimento o sull'esito del processo e non risulta che l'imputato abbia liberamente espresso il suo consenso alla domanda di assistenza giudiziaria». In una lettura sistematica delle fonti, assume particolare importanza ed autonomia la rilevanza penale dei fatti oggetto del procedimento, in applicazione del principio della doppia incriminazione.

⁶²² Cfr., J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 715.

Sebbene sembrino ricalcare quanto già previsto dalla disciplina interna dello Stato italiano, la dottrina ritiene che tali motivi di rifiuto costituiscano pur sempre ostacolo alla speditezza delle attività investigative o probatorie limitative di una efficace repressione della criminalità sovranazionale nel mondo contemporaneo⁶²³.

Vi è da chiedersi cosa intenda la Convenzione per interessi essenziali. La formulazione, non particolarmente chiara e felice, sembra voglia atteggiarsi a clausola di apertura. La vaghezza del concetto sembra lasciare ampia discrezionalità in capo a coloro i quali sono chiamati ad individuarli. Si potrebbe ritenere che gli Stati firmatari abbiano voluto far riferimento ai principi fondamentali dello Stato, nonché a quelli sanciti nella Dichiarazione per la salvaguardia dei diritti umani e delle libertà fondamentali e della Carta dei diritti fondamentali dell'UE, tra l'altro, entrambi richiamati all'art. 6 TUE.

I motivi di rifiuto potrebbero in ogni caso essere ordinati in quattro categorie: rilevanza penale, per l'applicazione del requisito della doppia incriminazione; tutela della sicurezza nazionale; impossibilità di natura oggettiva; violazione dei principi fondamentali⁶²⁴.

L'incisività con cui i motivi di rifiuto possono agire sull'esecuzione delle rogatorie relative alle *digital evidence* – seppur evidente – non può apparire espressione di una monade normativa interpretabile alla luce solo di quanto stabilito dall'art. 27, par. 4 della Convenzione. Invero, per una corretta lettura sistematica, non va dimenticato quanto stabilito dai principi generali sulla cooperazione giudiziaria. Se è vero che gli artt. 23 e 25 della Convenzione postulano il principio dell'ampia collaborazione, allora gli Stati dovrebbero esercitare il veto mediante i motivi di rifiuto in ipotesi ristrette e con moderazione. In pratica, la Convenzione richiede che quel potere, espressione della sovranità statale, non sia utilizzato sovente per negare categoricamente o per sottoporre a condizioni particolarmente onerose l'esecuzione delle rogatorie relative a prove elettroniche⁶²⁵.

Non dà luogo a motivo di rifiuto il pregiudizio per le indagini o i procedimenti condotti dalle autorità dello Stato richiesto, bensì è causa di sospensione dell'esecuzione della richiesta. È consentito, dunque, allo Stato richiesto di posticipare l'assistenza giudiziaria anziché rifiutarne drasticamente l'esecuzione⁶²⁶.

⁶²³ A simile conclusione giunge anche M. DANIELE, *Ricerca e formazione della prova*, cit., p. 458.

⁶²⁴ Per un approfondimento, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1624 ss.

⁶²⁵ In linea con questo approccio, si è inteso che, a parte i motivi di cui all'art. 28, il rifiuto dell'assistenza per motivi di protezione dei dati può essere invocato solo in casi eccezionali. Tale situazione potrebbe sorgere nelle ipotesi in cui, nel bilanciare gli interessi essenziali coinvolti nel caso particolare (da un lato, interessi pubblici, compresa la sana amministrazione della giustizia e, dall'altro, il diritto alla privacy), la cessione di specifici dati richiesti dalla Parte richiedente potrebbe sollevare difficoltà così importanti da lasciare spazio alla Parte richiesta per l'attivazione del motivo di rifiuto degli interessi essenziali. È dunque preclusa un'applicazione ampia, categorica o sistematica dei principi di protezione dei dati per rifiutare la cooperazione. Pertanto, il fatto che le parti interessate dispongano di sistemi diversi di protezione della privacy dei dati (ad esempio che la parte richiedente non dispone dell'equivalente di un'autorità specializzata per la protezione dei dati) o dispongano di mezzi diversi per proteggere i dati personali (è il caso della parte richiedente che utilizza mezzi diversi dal processo di cancellazione per proteggere la privacy o l'accuratezza dei dati personali ricevuti dalle autorità di contrasto) non costituiscono motivo di rifiuto. Prima di invocare "interessi essenziali" come base per rifiutare la cooperazione, la Parte richiesta dovrebbe invece tentare di porre condizioni che permettano il trasferimento dei dati. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 269, p. 48.

⁶²⁶ Cfr., art. 27, par. 5 della Convenzione sulla criminalità informatica. Ad esempio, se la Parte richiedente ha domandato elementi investigativi o informazioni da persone a conoscenza dei fatti a fini di indagine o per scopi processuali e gli stessi siano necessari per un processo che sta per iniziare nello Stato

Proiezione del principio di ampia collaborazione è quanto stabilito al paragrafo 6, il quale incentiva il dialogo tra le Parti, al fine di evitare sospensioni o rifiuti mediante l'esecuzione condizionata o l'esecuzione parziale. In tal caso, l'esecuzione è subordinata all'accettazione da parte dello Stato richiedente delle condizioni poste dallo Stato richiesto.

Ed invero, la Parte richiesta, prima di optare per la sospensione o il rifiuto dell'assistenza, deve valutare se può eseguire in parte la richiesta o sottoporla a condizione, eventualmente consultandosi con la Parte richiedente. Se le condizioni non sono gradite alla Parte richiedente, può modificarle, in un'ottica di continua e proficua collaborazione, al fine di salvaguardare con ogni mezzo la ricerca e formazione della prova elettronica ovvero esercitare il proprio diritto di rifiutare o posticipare l'assistenza.

È evidente come il principio di ampia collaborazione si manifesti sotto due aspetti: moderazione nell'esercizio dei motivi di rifiuto e delle condizioni; sollecitazione all'avvio del proficuo e costruttivo dialogo tra le Parti, per la salvaguardia di attività investigative e probatorie finalizzate al contrasto della criminalità informatica e, più in generale, all'efficiente funzionamento dei meccanismi di cooperazione.

Ai fini di un'ampia collaborazione, è previsto in capo allo Stato richiesto un obbligo di informativa nei confronti dello Stato richiedente per una leale collaborazione. La Parte richiesta deve "informare, motivando" la Parte richiedente dei profili relativi alla mancata esecuzione per impossibilità o della ritardata esecuzione. È inoltre obbligata ad informare l'altra Parte dell'esito delle richieste, indicando le ragioni del rifiuto o della sospensione⁶²⁷.

La motivazione ha un ruolo centrale nei rapporti tra autorità straniere, perché assume una funzione cognitiva e pedagogica, in quanto rappresenta il mezzo con il quale gli Stati capiscono come le altre Parti interpretano i requisiti dettati dall'art. 27 e forniscono una base per le consultazioni al fine non solo di migliorare l'efficienza futura dell'assistenza reciproca, ma anche di dotare la Parte richiedente di informazioni fattuali precedentemente sconosciute⁶²⁸.

Una volta superato il vaglio di ammissibilità, si apre la fase dell'esecuzione, dedicata alla ricerca e formazione nonché al trasferimento degli elementi aventi attitudine probatoria. La Convenzione non individua modalità o protocolli applicativi per la ricerca e formazione, ma formula solo obiettivi. La dottrina ritiene saggia tale scelta perché risponde al meglio alla «rapida ed incessante evoluzione che contraddistingue l'informatica, ma che al contempo ha come conseguenza l'assenza di sanzioni»⁶²⁹.

La Convenzione prescrive l'applicazione della *lex fori*, in deroga a quanto indica il principio strutturale della mutua assistenza, che generalmente segue la regola del *locus*

richiesto, la Parte richiesta potrà motivarne così il rinvio. Sul punto, anche, C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cibercriminalità*, cit., p. 512.

⁶²⁷ Cfr., art. 27, par. 7, Convenzione del Consiglio d'Europa sulla criminalità informatica.

⁶²⁸ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 272, p. 49.

⁶²⁹ Secondo tale orientamento, non sarebbero configurabili nullità o inutilizzabilità quando le operazioni non sono svolte da esperti o quando sono utilizzate tecniche che non assicurino le finalità perseguite dal legislatore. In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1627. L'A. ritiene che «l'unico antidoto alla fallibilità delle indagini informatiche è costituito dal contraddittorio: il quale in questo caso si concretizza nella possibilità per la difesa di partecipare alla raccolta delle prove digitali con i propri consulenti, con la facoltà di questi ultimi di contrapporsi dialetticamente ai consulenti dell'accusa». In senso opposto, L. LUPÀRIA, *Computer crimes e procedimento penale*, in AA.VV., *Modelli differenziati di accertamento* (a cura di G. GARUTI), Tomo I, Torino, 2011, p. 389 ss.; L. MARAFIOTI, *Digital evidence e processo penale*, cit., p. 4521 ss.

regit actum. Invero, ai sensi dell'art. 27, comma 3, della Convenzione, le richieste devono essere eseguite «in conformità alle procedure specificate dalla Parte richiedente». L'obiettivo sarebbe quello di consentire allo Stato richiedente di garantire l'utilizzabilità delle prove formate dinanzi ai suoi tribunali⁶³⁰. Tuttavia, dovrebbe parlarsi di *lex fori* "temperata" poiché essa può essere applicata solo se compatibile con la legislazione della Parte richiesta. La scelta, dunque, rappresenterebbe una soluzione "ibrida" tra l'applicazione della *lex loci* e il criterio della *lex fori*.

La scelta della *lex fori* rappresenta un'evoluzione ed una rivoluzione per i modelli basati sulla mutua assistenza. Sarebbe concreta applicazione del principio di ampia cooperazione, espressione di un maggiore livello di fiducia reciproca acquisita tra gli Stati che hanno ratificato la Convenzione e proiezione della consapevolezza raggiunta della necessità di un sistema di cooperazione che sia quanto più rapido possibile e dai tempi ragionevolmente contenuti, in relazione al particolare tipo di prova da formare.

L'esegesi della norma è tutt'altro che evidente. Ci si chiede cosa bisogna intendere per "procedure specificate" e per "incompatibilità con la legislazione della Parte richiesta". Si ritiene che le procedure siano riferibili ad un obbligo di rispettare i requisiti procedurali tecnici, non tutele procedurali fondamentali⁶³¹. Di conseguenza, per "legislazione della Parte richiesta" la Convenzione farebbe riferimento ai principi fondamentali del diritto dello Stato di esecuzione⁶³². Pertanto, ad esempio, uno Stato richiedente non potrebbe richiedere di eseguire una perquisizione o un sequestro con modalità che non soddisfino i requisiti posti dai diritti fondamentali dello Stato richiesto⁶³³.

Oltre alle regole dettate dalla Convenzione di Budapest, assumono rilevanza le norme del codice di procedura penale, nel caso in cui l'Italia sia la Parte richiesta. Sarebbero essenzialmente prescrizioni che mirano a salvaguardare i diritti fondamentali degli interessati⁶³⁴. Inoltre, l'art. 725 c.p.p., in un'ottica di dialogo tra autorità, consente al procuratore della Repubblica di informare senza ritardo l'autorità richiedente per l'integrazione della richiesta, qualora rilevi l'opportunità del compimento di atti ulteriori non indicati nella richiesta, nel corso dell'esecuzione⁶³⁵.

⁶³⁰ In tal senso, M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 319.

⁶³¹ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 267, p. 48.

⁶³² M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1628.

⁶³³ Alla luce della natura limitata dell'obbligo, si è convenuto che il semplice fatto che il sistema giuridico della Parte richiesta non conosca tale procedura non è un motivo sufficiente per rifiutare di applicare la procedura richiesta dalla Parte richiedente; invece, per il rifiuto, la procedura deve essere incompatibile con i principi giuridici della Parte richiesta. Ad esempio, in base alla legge della Parte richiedente, può essere un requisito procedurale che una dichiarazione di un testimone sia resa sotto giuramento. Anche se la Parte richiesta a livello nazionale non ha l'obbligo di rendere le dichiarazioni sotto giuramento, si dovrebbe comunque eseguire la richiesta. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 267, p. 48.

⁶³⁴ In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1627.

⁶³⁵ Il codice ammette anche forme di partecipazione all'esecuzione dell'atto richiesto, come la "rogatoria concelebrata". Invero, nel caso di rogatoria dall'estero, l'art. 725, comma 3, c.p.p. consente all'autorità giudiziaria di autorizzare, con decreto motivato, la presenza al compimento degli atti richiesti di rappresentanti o incaricati dell'autorità richiedente. Analogamente, in caso di rogatoria all'estero, la giurisprudenza ritiene che «L'art. 727 cod. proc. pen. - che prevede la rogatoria internazionale per l'attività di acquisizione probatoria all'estero - non impedisce che, con il consenso delle autorità dello Stato straniero, le prove siano raccolte direttamente dall'autorità giudiziaria italiana». Cfr., Cass., Sez. V, sentenza del 5 febbraio 1997, n. 873, in *CED Cass.*, rv. 206902. In senso conforme, Cass., Sez. VI, sentenza del 30 gennaio

Quanto ai tempi, la volatilità delle prove elettroniche richiede che questi siano quanto più contenuti possibile. I classici strumenti rogatoriali basati sul principio della mutua assistenza sono lenti e ricchi di sovrastrutture. Sebbene la Convenzione sulla criminalità informatica prova ad accelerare le operazioni di ricerca e formazione delle prove elettroniche, l'obiettivo non sembra che venga spesso raggiunto, nonostante l'art. 31 e – più in generale – l'art. 35 della Convenzione di Budapest tentino di dare una decisa accelerazione alle attività rispetto agli altri strumenti di assistenza.

È evidente come sia necessario individuare il miglior equilibrio tra due contrapposte esigenze: da una parte vi è la necessità di favorire la cooperazione internazionale in materia penale, attraverso il superamento di formalismi superflui e l'agevolazione dello scambio di informazioni ed atti tra autorità giudiziarie straniere; dall'altra vi sono i principi ed i diritti fondamentali da salvaguardare soprattutto nel momento di apprensione del dato avente carattere probatorio⁶³⁶.

Dopo la formazione, la prova è trasferita nello Stato richiedente⁶³⁷.

L'ultima fase è relativa all'utilizzabilità della prova. Innanzitutto, si ritiene che talune regole di esclusione delle prove digitali raccolte all'estero possano considerarsi implicite nella normativa sovranazionale sulla rogatoria, potendosi rinvenirle nel caso della violazione delle regole di ammissibilità delle prove operanti a livello nazionale, ossia dei requisiti stabiliti a pena di invalidità nei processi interni ai fini delle ispezioni, delle perquisizioni e dei sequestri informatici⁶³⁸.

Come già chiarito, la ricerca e formazione della prova informatica avviene secondo la *lex fori*; pertanto, l'autorità di emissione indica all'autorità di esecuzione le regole da

2002, n. 3383, in *CED Cass.*, rv. 220633. In dottrina, S. ASTARITA, *Vecchio e nuovo in tema di rogatorie internazionali*, cit., p. 150 ss.; G. DARAIO, *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), cit., p. 1083 ss.; ID., *Le rogatorie internazionali*, cit., p. 681 ss.; G. DI PAOLO, *La riforma della disciplina codicistica delle rogatorie internazionali (D.Lg. 3 ottobre 2017, n. 149)*, cit., p. 3425; G. DIOTALLEVI, *La c.d. «concelebrazione» delle rogatorie e gli atti diretti di giurisdizione all'estero*, in *Cass. pen.*, 3, 1998, p. 913 ss.; I. IAI, *Rogatoria eseguita all'estero dall'autorità giurisdizionale dello Stato richiedente*, cit., p. 1471 ss.; J.P. PIERINI, *Ancora attuale il principio locus regit actum con riguardo alle prove penali acquisite all'estero nel corso di rogatoria «concelebrata»?*, cit., p. 3106 ss.; M. PISANI, *In tema di assunzione all'estero delle prove da parte dell'autorità giudiziaria italiana*, in *Riv. it. dir. e proc. pen.*, 2001, p. 557 ss.; D. VIGONI, *Dalla rogatoria all'acquisizione diretta*, in AA.VV., *Rogatorie penali e cooperazione giudiziaria internazionale* (a cura di G. LA GRECA, M.R. MARCHETTI), Torino, 2003, p. 417 ss.

⁶³⁶ Così, A. COLAIOCCO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. pen.*, 1, 2019, p. 5.

⁶³⁷ Qualora lo Stato richiedente sia l'Italia, deve rammentarsi che i documenti acquisiti all'estero mediante rogatoria internazionale, i verbali degli atti non ripetibili assunti con le stesse modalità nonché i verbali degli atti diversi da questi assunti all'estero a seguito di rogatoria internazionale ai quali i difensori sono stati posti in grado di assistere e di esercitare le facoltà loro consentite dalla legge italiana sono raccolti nel fascicolo delle indagini preliminari e, ai sensi dell'art. 431 c.p.p., immediatamente dopo l'emissione del decreto che dispone il giudizio, sono inseriti nel fascicolo del dibattimento. Inoltre, la giurisprudenza ritiene che sia legittima l'acquisizione al fascicolo del dibattimento di atti di provenienza estera di natura amministrativa, compiuti al di fuori di una specifica indagine penale, che in quanto tali non possono considerarsi sottoposti al regime proprio delle rogatorie internazionali. Cfr., *Cass.*, Sez. II, sentenza del 20 gennaio 2015, n. 2471, in *Ced Cass.*, rv. 261822; *Cass.*, Sez. VI, sentenza del 23 luglio 2012, n. 30068, in *Ced Cass.*, rv. 253273.

⁶³⁸ In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1630.

rispettare a pena di invalidità secondo le leggi interne⁶³⁹, oltre alle norme inderogabili dell'ordinamento relative all'ordine pubblico o al buon costume.

È discusso se il mancato rispetto delle *best practices* richieste a livello nazionale possa essere sanzionato con l'inutilizzabilità ovvero possa costituire una mera "irregolarità" ed essere valutato dal giudice ai fini dell'attendibilità. Secondo un primo orientamento, l'inosservanza dei protocolli relativi alla formazione della prova digitale non causerebbe l'inutilizzabilità dei risultati⁶⁴⁰. Diversamente, altro orientamento ritiene che l'inosservanza delle *best practices* ne determinerebbe l'inutilizzabilità⁶⁴¹.

Nel caso in cui l'Italia sia lo Stato di emissione, è necessario che l'autorità di emissione descriva «modalità e forme stabilite dalla legge ai fini dell'utilizzabilità degli atti richiesti»⁶⁴². Qualora le regole non siano rispettate dallo Stato estero di esecuzione, gli atti compiuti sono inutilizzabili in ogni stato e grado del procedimento solo nei casi in cui la sanzione – rilevabile anche d'ufficio – sia prevista per legge⁶⁴³.

L'art. 28 della Convenzione sulla criminalità informatica consente alla Parte richiesta di subordinare la trasmissione di informazioni o materiali in risposta ad una richiesta a due condizioni. Si tratterebbe della previsione di due clausole di limitazione d'uso con le quali lo Stato di esecuzione pone un veto sull'utilizzo di informazioni o materiale, nei casi in cui tali informazioni o materiali siano particolarmente sensibili.

Con l'apposizione di tali clausole, si garantisce che l'uso delle informazioni o del materiale sia limitato a quello per cui è concessa l'assistenza ovvero che non sia divulgato oltre i funzionari delle forze dell'ordine della Parte richiedente. Queste restrizioni forniscono garanzie che sono disponibili, tra l'altro, per scopi di protezione dei dati⁶⁴⁴.

Lo Stato richiesto potrebbe richiedere o un obbligo di riservatezza o un divieto d'uso extraprocedimentale.

Con l'obbligo di riservatezza previsto all'art. 28, par. 2, lett. a., della Convenzione sulla criminalità informatica, la Parte richiesta impone allo Stato di emissione di mantenere confidenziali le informazioni o i materiali da ricevere. Tale clausola risulta

⁶³⁹ Così, A. COLAIOCCO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, cit., p. 6 ss.

⁶⁴⁰ La giurisprudenza ha chiarito che l'estrazione di dati archiviati in un supposto informatico non costituisce accertamento tecnico irripetibile anche dopo l'entrata in vigore della legge 18 marzo 2008, n. 48, che ha introdotto unicamente l'obbligo per la polizia giudiziaria di rispettare determinati protocolli di comportamento, senza prevedere alcuna sanzione processuale in caso di mancata loro adozione, potendone derivare, invece, eventualmente, effetti sull'attendibilità della prova rappresentata dall'accertamento eseguito. Sul tema, Cass., Sez. V, sentenza del 21 marzo 2016, n. 11905, in *Ced Cass.*, rv. 266477. V., anche, Cass., Sez. II, sentenza dell'8 luglio 2015, n. 29061, in *Ced Cass.*, rv. 264572. In dottrina, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1630.

⁶⁴¹ In tal senso, M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., p. 159, secondo il quale le *best practices* sarebbero canoni di genuinità e non alterazione della prova legislativamente imposti dalla l. 18 marzo 2018, n. 48, pertanto non sono «mere indicazioni operative prive di alcuna sanzione, ma veri e propri divieti impliciti presidiati dalla sanzione dell'inutilizzabilità». V., anche, C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, in *Cass. pen.*, 2, 2013, p. 485 ss., secondo la quale le regole dettate dalle l. 48/2018 sarebbero «regole di esclusione *sui generis* che parlano un linguaggio scientifico e costituiscono un inedito parametro di legalità della prova».

⁶⁴² Art. 727, comma 9, c.p.p.

⁶⁴³ Art. 729, comma 2, c.p.p. In ogni caso, ai sensi dell'art. 729, comma 3, c.p.p. non possono essere utilizzate le dichiarazioni, da chiunque rese, aventi ad oggetto il contenuto di atti inutilizzabili.

⁶⁴⁴ *Explanatory Report to the Convention on Cybercrime*, par. 275, p. 49.

necessaria qualora la richiesta non possa essere soddisfatta in assenza di tale condizione⁶⁴⁵.

Il divieto d'uso extraprocedimentale, invece, consente alla Parte richiesta di subordinare l'utilizzo delle informazioni o dei materiali alla condizione che non vengano utilizzati per indagini o procedimenti diversi da quelli indicati nella richiesta⁶⁴⁶.

Sembra siano riconosciute implicitamente due eccezioni alle clausole di limitazione d'uso. In primo luogo, in base ai principi giuridici fondamentali di molti Stati, se il materiale fornito è una prova a discarico di una persona accusata, deve essere divulgato alla difesa o all'autorità giudiziaria. In secondo luogo, la maggior parte del materiale fornito nell'ambito dei regimi di assistenza giudiziaria è destinato all'uso durante il processo, normalmente pubblico, ove la divulgazione delle informazioni è obbligatoria. Una volta che tale divulgazione ha avuto luogo, il materiale è passato essenzialmente al pubblico dominio. In queste situazioni non è possibile garantire la riservatezza alle indagini o ai procedimenti per i quali è stata richiesta l'assistenza reciproca⁶⁴⁷.

Poste condizioni all'utilizzabilità degli atti richiesti, l'autorità giudiziaria è vincolata al rispetto di esse, secondo la regola di specialità⁶⁴⁸. Potrebbe accadere però che la Parte richiedente non possa soddisfare una delle condizioni. Innanzi a tali circostanze, la Convenzione – nello spirito della più ampia collaborazione – consente alle Parti di avviare un dialogo che porti per quanto possibile ad una soluzione proficua e costruttiva, che sia ragionevole in termini di sicurezza pubblica e tutela dei diritti fondamentali.

Ed invero, l'art. 28, par. 3, della Convenzione sulla criminalità informatica impone alla Parte richiedente che non possa soddisfare la condizione apposta di notificare prontamente all'altra parte l'impossibilità ad adempiere, al fine di stabilire se l'informazione possa essere comunque trasmessa e secondo quali condizioni alternative. Infatti, la Parte richiesta, in assenza di accordo, potrebbe non consentire il trasferimento delle informazioni o del materiale. Tuttavia, accettata la condizione, lo Stato richiedente dovrà attenersi.

Nel pieno rispetto delle parti, nel dar corso ad un costante confronto tra loro, lo Stato richiesto potrebbe anche richiedere all'altro Paese precisazioni relative al rispetto delle condizioni ovvero al futuro impiego delle informazioni o del materiale⁶⁴⁹.

⁶⁴⁵ Ad esempio, quando è coinvolta l'identità di un informatore riservato. Secondo l'*Explanatory Report to the Convention on Cybercrime*, par. 277, p. 49 ss., non è opportuno richiedere la riservatezza assoluta nei casi in cui la Parte richiesta è obbligata a fornire l'assistenza richiesta, poiché ciò, in molti casi, ostacolerebbe la capacità della Parte richiedente di indagare o perseguire con successo il crimine, ad es. utilizzando le prove in un processo pubblico (compresa la divulgazione obbligatoria).

⁶⁴⁶ Affinché questa condizione si applichi, deve essere espressamente invocata dalla Parte richiesta, altrimenti non vi è alcuna limitazione di utilizzo da parte della Parte richiedente. Nei casi in cui venga invocata, tale condizione garantirà che le informazioni e il materiale possano essere utilizzati solo per le finalità previste nella richiesta, escludendo così l'uso del materiale per altri scopi senza il consenso della Parte richiesta.

⁶⁴⁷ *Explanatory Report to the Convention on Cybercrime*, par. 278, p. 50.

⁶⁴⁸ Cfr., art. 729, comma 1, c.p.p. La regola di specialità, corollario del principio per cui ogni Stato ha il potere sovrano di regolare l'esecuzione di atti giurisdizionali sul proprio territorio e del divieto di ingerenza per gli altri Stati di esercitare il potere giurisdizionale sul suolo straniero, stabilisce che la prova acquisita mediante rogatoria non possa essere utilizzata dallo Stato richiedente in procedimenti diversi da quello per il quale è stata richiesta. Sul punto, A. COLAIOCCO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, cit., p. 6.

⁶⁴⁹ Art. 28, par. 4, Convenzione sulla criminalità informatica. È stato convenuto che la Parte richiesta non può richiedere una contabilità eccessivamente onerosa, ad esempio ogni volta che si accede al materiale o alle informazioni fornite. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 280, p. 50.

Le spiegazioni richieste hanno una chiara finalità accertativa. La funzione di controllo assunta dallo scambio di informazioni risulta fondamentale per saldare una fiducia reciproca non presupposta con gli strumenti basati sul principio della mutua assistenza.

Infine, l'art. 27, par. 9, della Convenzione sulla criminalità informatica prevede una procedura particolarmente rapida e snella, molto simile agli schemi strutturalmente previsti con il principio del mutuo riconoscimento, così da poter parlare di attenuata applicazione del principio della mutua assistenza.

Solo in casi di urgenza, è previsto che le richieste di mutua assistenza o le comunicazioni collegate possano essere trasmesse senza l'ausilio dei classici sistemi rogatoriali di comunicazione, ma attraverso il diretto contatto tra autorità giudiziarie⁶⁵⁰.

Invero, le richieste di assistenza giudiziaria reciproca possono essere inviate, anche con l'assistenza dell'Organizzazione Internazionale della Polizia Criminale (Interpol)⁶⁵¹,

⁶⁵⁰ La Convenzione ha previsto la possibilità per le Parti, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, di comunicare al Segretario Generale del Consiglio d'Europa che, per ragioni di efficienza, le richieste effettuate in base al paragrafo 9 dovranno essere indirizzate alla propria autorità centrale.

⁶⁵¹ L'Organizzazione internazionale di polizia criminale (INTERPOL) è un'organizzazione internazionale di cui fanno parte 194 Paesi. Interpol svolge una funzione di supporto alla polizia di tutti gli Stati membri, per finalità di sicurezza. Consente loro di condividere e accedere ai dati sui crimini e sui criminali e offre supporto tecnico ed operativo. Obiettivo di INTERPOL è consentire alla polizia di tutto il mondo di collaborare per prevenire e combattere la criminalità internazionale. Essa offre alla polizia un'infrastruttura *high-tech* di supporto tecnico e operativo per far fronte alle crescenti sfide poste da criminali e crimini transnazionali e informatici.

È composto da un Segretariato generale, da un Ufficio centrale nazionale (BCN) dell'Interpol e dall'Assemblea generale. Il segretariato generale coordina le attività ed è gestito da un segretario generale. Il segretariato è formato da membri afferenti alla polizia e da civili, ed ha sede a Lione, mentre l'*INTERPOL Global Complex for Innovation* (IGCI) ha sede a Singapore. Esistono anche diversi uffici satellite in molte regioni internazionali.

In ogni Stato, l'Ufficio centrale nazionale dell'Interpol fornisce un punto di contatto centrale per il Segretariato generale e per le altre BCN. Le BCN sono generalmente gestite da funzionari della polizia nazionale e di solito è membro anche il ministro responsabile della polizia.

L'Assemblea generale è l'organo di governo e riunisce tutti i Paesi una volta all'anno per prendere decisioni. Ha lo scopo di garantire che le attività di INTERPOL corrispondano alle esigenze dei Paesi membri, attraverso la determinazione dei principi e delle misure necessarie per raggiungere gli obiettivi e rivedendo e approvando il programma di attività e la politica finanziaria per l'anno successivo. Inoltre, elegge i membri del Comitato Esecutivo, l'organo di governo con funzioni di direzione delle sessioni dell'Assemblea. Ogni anno all'ordine del giorno ci sono anche le principali tendenze della criminalità e le minacce alla sicurezza che il mondo deve affrontare.

INTERPOL collega tutti i Paesi tramite un sistema di comunicazione chiamato I-24/7. I Paesi utilizzano questa rete sicura per contattarsi l'un l'altro, nonché per rivolgersi al Segretariato generale. Inoltre, consente loro di accedere ai *database* e ai servizi in tempo reale, sia da postazioni centrali che remote. L'organizzazione coordina anche reti di polizia ed esperti in diverse aree della criminalità, che si riuniscono attraverso gruppi di lavoro e in conferenze per condividere esperienze e idee.

Il Segretariato generale fornisce una gamma di competenze e servizi ai Paesi membri, attraverso la gestione di 18 *database* di polizia con informazioni su crimini e criminali (da nomi e impronte digitali a passaporti rubati), accessibili in tempo reale ai Paesi. Inoltre, offre supporto investigativo e forense, analisi e assistenza nella localizzazione di latitanti in tutto il mondo. Ampia rilevanza è data alla formazione in molte aree, in modo che i funzionari sappiano come lavorare in modo efficiente con i servizi offerti.

Questa esperienza supporta gli sforzi nazionali nella lotta ai crimini in tre aree globali considerate di particolare allarme: terrorismo, criminalità informatica e criminalità organizzata. Invero, INTERPOL assiste gli Stati nella lotta alla criminalità: attraverso la prevenzione e interruzione di attività terroristiche, identificando i membri delle reti terroristiche e dei loro affiliati, nonché contrastando i principali fattori che consentono la loro attività: viaggi, diffusione dei contenuti *online*, circolazione di armi, materiali e finanziamento illegale; mediante attività di repressione della cibercriminalità; attraverso lo smantellamento

direttamente dai giudici e dagli uffici del pubblico ministero della Parte richiedente ai giudici e agli uffici del pubblico ministero della Parte richiesta. Il giudice o l'ufficio del pubblico ministero che segue questa procedura deve anche inviare una copia della richiesta presentata alla propria autorità centrale in vista della sua trasmissione all'autorità centrale della Parte richiesta⁶⁵².

In caso di propria incompetenza, l'autorità giudiziaria della parte richiesta deve trasferire la domanda all'autorità competente, informando prontamente le autorità della Parte richiedente del trasferimento effettuato. La norma nulla stabilisce in caso di conflitto negativo o contrasto tra uffici. In Italia, dovendosi ritenere che l'autorità giudiziaria legittimata a cui inviare direttamente le richieste sia sempre l'ufficio del pubblico ministero, dovrebbe applicarsi la disciplina prevista agli artt. 54 e 54-ter c.p.p.

La procedura appena descritta è attivabile anche se non vi sia urgenza, purché l'autorità della Parte richiesta sia in grado di ottemperare alla richiesta senza ricorrere a un'azione coercitiva. Infatti, l'art. 27, par. 9, lett. d. consente che «Le richieste o le comunicazioni effettuate in base a questo paragrafo che non implicino azioni coercitive possono essere direttamente trasmesse dalle autorità competenti della Parte richiedente alle autorità competenti della Parte richiesta».

Discorso a parte merita il tema delle investigazioni difensive all'estero. Nonostante la giurisprudenza in passato abbia compreso le facoltà difensive⁶⁵³, la dottrina ritiene che debba essere concessa una maggior attenzione al diritto di difesa mediante il pieno rispetto del principio di proporzionalità⁶⁵⁴.

Si ritiene che il difensore possa svolgere indagini difensive mediante il sistema della "canalizzazione". La giurisprudenza di legittimità, con una tesi ritenuta ardita dalla dottrina, ha affermato che presupposto per l'utilizzabilità degli atti di investigazione difensiva compiuti all'estero sia l'assunzione di questi a seguito dell'espletamento della procedura prevista in tema di rogatoria. Di talché, deriverebbe la necessità per il difensore di canalizzare la richiesta di ricerca e formazione della prova all'ufficio del pubblico ministero ovvero al giudice per le indagini preliminari, non disponendo di un diretto potere di sollecitazione della procedura rogatoria⁶⁵⁵.

delle organizzazioni transnazionali delle reti criminali nonché l'identificazione, l'analisi e la risposta alle minacce emergenti.

I funzionari che lavorano in ciascuna area criminale specializzata gestiscono una serie di attività diverse insieme ai paesi membri. Può trattarsi di supporto investigativo, operazioni sul campo, formazione e *networking*. È importante sottolineare che, poiché i crimini si evolvono, l'INTERPOL è attenta al futuro attraverso la ricerca e lo studio della criminalità e delle tendenze internazionali.

In quanto organizzazione internazionale, fornisce una piattaforma per la cooperazione, consentendo alla polizia di lavorare direttamente con le loro controparti, anche tra Paesi che non hanno relazioni diplomatiche.

⁶⁵² Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 274, p. 49.

⁶⁵³ Cfr., Cass., Sez. I, sentenza del 5 dicembre 2002, n. 41005, in *Ced Cass.*, rv. 223202. V., inoltre, Cass., Sez. VI, sentenza del 18 novembre 2004, n. 44830, in *Ced Cass.*, rv. 230594; Cass., Sez. I, sentenza del 25 gennaio 2008, n. 4060, in *Ced Cass.*, rv. 239193; Cass., SS.UU., sentenza del 25 febbraio 2010, n. 15208, punto 10.3.

⁶⁵⁴ Così, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1630 ss.

⁶⁵⁵ In tal senso, Cass., Sez. I, sentenza del 29 maggio 2007, n. 23967, in *Ced Cass.*, rv. 236594. In dottrina, C. ANGELONI, *L'inammissibilità di investigazioni difensive all'estero: una ricostruzione plausibile?*, in *Riv. it. dir. e proc. pen.*, 3, 2008, p. 1384 ss., ove si afferma che l'inutilizzabilità delle investigazioni difensive «discende dai principi generali del codice di procedura penale e, pur non essendo esplicitamente affermato che il difensore non può recarsi all'estero a svolgere dette investigazioni, discende dall'ordinamento tale divieto, essendo evidente che, ai fini dell'utilizzabilità di atti compiuti all'estero, per

Tuttavia, questo meccanismo produce una preventiva *discovery* delle risultanze investigative difensive che potrebbero di fatto ledere il diritto di difesa e il principio della parità delle armi⁶⁵⁶. Pertanto, sembra consentito alla parte svolgere autonomamente le proprie attività all'estero.

Ed invero, la giurisprudenza ha stabilito che la sanzione dell'inutilizzabilità degli atti assunti per rogatoria non si applica ai documenti acquisiti in via autonoma dalla parte all'estero direttamente dalle amministrazioni competenti⁶⁵⁷.

Sul punto, va osservato che né la Convenzione sulla criminalità informatica, né la disciplina codicistica dettano regole. Invero, il legislatore non ha agito nel senso di esplicitare la procedura di formazione della prova richiesta dal difensore, nell'ipotesi in cui questi si trovi a dover svolgere l'attività investigativa al di fuori dei confini nazionali. Da qui, nascono interrogativi intorno al diritto di difendersi, ricercando la prova all'estero.

In assenza di un espresso divieto di legge, è stato sostenuto che il difensore, nello svolgimento di una funzione di natura privatistica⁶⁵⁸, è legittimato a svolgere attività investigativa anche in un altro Stato⁶⁵⁹, senza necessità di attivare la procedura rogatoria, con il solo limite degli atti d'indagine che richiedano l'esercizio di poteri coercitivi o la partecipazione necessaria del pubblico ministero⁶⁶⁰.

tutte le parti processuali, deve essere esperita la procedura prevista dal codice in materia di rogatorie». Particolarmente critico anche D. CURTOTTI NAPPI, *I nuovi orizzonti investigativi del difensore: le informazioni assunte all'estero*, in *Giur. It.*, 4, 2008, p. 987 ss., secondo la quale un simile orientamento incide non solo sul diritto di difesa ma anche sul principio di uguaglianza. V., anche, F. ALBANO, *Sui limiti territoriali delle indagini difensive: note a margine di una discutibile pronuncia*, in *Cass. pen.*, 12, 2008, p. 4708B ss.; G. BIONDI, *La giurisprudenza in tema di investigazioni difensive, con particolare riferimento all'attività di assunzione di informazioni*, in *Giur. Merito*, 4, 2008, p. 923B ss.; M. BORDIERI, *Brevi note sull'inutilizzabilità di atti di investigazione svolti all'estero dal difensore dell'imputato senza passare attraverso una rogatoria internazionale*, in *Cass. pen.*, 5, 2009, p. 2035 ss.

⁶⁵⁶ Evidenzia questa disparità di trattamento tra le parti, N. TRIGGIANI, *Le investigazioni difensive*, Milano, 2002, p. 225.

⁶⁵⁷ Così, Cass., Sez. II, sentenza del 31 gennaio 2020, n. 4152, in *Ced Cass.*, rv. 278003. Nello specifico, è stata ritenuta legittima l'acquisizione, tramite indagini difensive svolte dalla parte civile, di documenti provenienti da società ed autorità doganali estere. Per un commento, V.M. THELMA, *Elementi probatori acquisiti dal privato in territorio straniero*, in *Proc. pen. e giust.*, 5, 2020, p. 1073. V., anche, Cass., Sez. III, sentenza del 27 maggio 2009, n. 24653, in *Ced Cass.*, rv. 244087.

⁶⁵⁸ Di questo avviso, G. BIONDI, *La giurisprudenza in tema di investigazioni difensive, con particolare riferimento all'attività di assunzione di informazioni*, cit., p. 926B; M.R. MARCHETTI, *L'assistenza giudiziaria internazionale*, cit., p. 128, la quale osserva come il difensore potrebbe compiere attività investigativa «eventualmente affiancato da un legale del luogo».

⁶⁵⁹ Così, A. MANGIARACINA, *Ancora zone d'ombra in tema di ammissibilità della revisione e indagini difensive svolte all'estero*, in *Giur. It.*, 5, 2009, p. 1244 ss.

⁶⁶⁰ Secondo C. ANGELONI, *L'inammissibilità di investigazioni difensive all'estero: una ricostruzione plausibile?*, cit., p. 1391, il difensore dovrebbe ricorrere allo strumento della rogatoria per potere effettuare all'estero una serie di atti, tra cui accertamenti tecnici irripetibili; atti non ripetibili in occasione dell'accesso ai luoghi ai quali il magistrato del Pubblico ministero ha diritto di assistere (art. 391-*decies*, comma 3, ult. parte, c.p.p.); audizione della persona in grado di riferire circostanze utili che si sia avvalsa della facoltà di non rispondere (art. 391-*bis*, commi 10 e 11, c.p.p.); rilascio di documenti che la pubblica amministrazione abbia negato (art. 391-*quater*, comma 3, c.p.p.); accesso ai luoghi privati o non aperti al pubblico, qualora manchi il consenso dell'interessato (art. 391-*septies* c.p.p.).

4. L'oggetto della domanda di assistenza giudiziaria

La sezione II del capitolo III della Convenzione sulla criminalità informatica fornisce meccanismi specifici al fine di intraprendere un'azione internazionale efficace e concertata nei casi che coinvolgono reati informatici e prove in forma elettronica.

Si tratta di un insieme di disposizioni specifiche che si concentrano sull'oggetto della domanda di assistenza giudiziaria, divisibili in due settori: disposizioni relative all'adozione di misure provvisorie⁶⁶¹ e disposizioni che regolano vere e proprie attività d'indagine⁶⁶². Entrambe presuppongono la preventiva localizzazione del dato informatico che si intende acquisire⁶⁶³.

Sono misure provvisorie: la conservazione rapida di dati informatici immagazzinati e la divulgazione rapida di dati di traffico conservati.

Con la conservazione rapida dei dati informatici contenuti in un sistema informatico, l'art. 29 introduce la tecnica del *data freezing*⁶⁶⁴, ossia un meccanismo di congelamento dell'elemento immateriale contenuto in un sistema informatico⁶⁶⁵. La misura deve essere

⁶⁶¹ Contenute nel titolo I, agli artt. 29 e 30.

⁶⁶² Titolo II, artt. 31-34.

⁶⁶³ Così, F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 185.

⁶⁶⁴ M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 319; A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, cit., p. 4.

⁶⁶⁵ L'articolo prevede un meccanismo a carattere transfrontaliero equivalente a quello previsto dall'articolo 16 per l'uso nazionale interno. L'art. 16 della Convenzione sulla criminalità informatica disciplina la conservazione rapida di dati informatici immagazzinati, il cui sistema informatico sia presente sul territorio in cui le autorità nazionali esercitano la propria giurisdizione. Ai sensi dell'art. 16 della Convenzione sulla criminalità informatica, «1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle competenti autorità di ordinare o ottenere in altro modo la protezione rapida di specifici dati informatici, inclusi i dati sul traffico, che sono stati conservati attraverso un sistema informatico, in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente vulnerabili e soggetti a cancellazione o modificazione.

2. Quando una Parte rende effettive le previsioni di cui al precedente paragrafo 1. attraverso l'ordine ad un soggetto di conservare specifici dati informatici immagazzinati che siano in suo possesso o sotto il suo controllo, la Parte deve adottare le misure legislative e di altra natura che siano necessarie per obbligare tale soggetto a proteggere e mantenere l'integrità di quei dati informatici per il periodo di tempo necessario, per un massimo di novanta giorni, per consentire alle autorità competenti di ottenere la loro divulgazione. Una Parte può prevedere che tale ordine possa essere successivamente rinnovato.

3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per obbligare il custode o la persona incaricata di conservare i dati informatici di mantenere il segreto sulla procedura intrapresa per il periodo di tempo previsto dal proprio diritto interno.

4. I poteri e le procedure di cui al presente articolo devono essere soggetti agli articoli 14 e 15».

In Italia, l'art. 16 è stato recepito con l. 18 marzo 2008, n. 48, la quale è intervenuta sul comma 2 dell'art. 354 c.p.p., relativo agli accertamenti urgenti su luoghi, cose e persone ad iniziativa della polizia giudiziaria, specificando che quando l'attività di accertamento ha ad oggetto informazioni, programmi o dati informatici, gli ufficiali di polizia giudiziaria devono attivarsi affinché questi non siano alterati prevedendo anche, ove possibile, la loro duplicazione. In particolare, «Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità». Sul tema, R.M.F. BARON, *A Critique of the*

mantenuta per un periodo non inferiore a sessanta giorni, prodromica all'eventuale successiva richiesta di perquisizione, sequestro o analogo strumento di ricerca della prova, nonché di divulgazione dei dati⁶⁶⁶. Si tratta di un termine "dilatorio", ossia un periodo minimo ritenuto congruo per permettere alla Parte richiedente di disporre del tempo necessario per effettuare la propria richiesta formale di assistenza giudiziaria. Inoltre, è previsto che i dati continuino ad essere conservati dopo il ricevimento della richiesta⁶⁶⁷.

Mentre il paragrafo 1, con una clausola a fattispecie aperta, autorizza una Parte a richiedere ad un altro Stato di ordinare od ottenere in altro modo la conservazione rapida di dati contenuti in un sistema informatico collocato nel territorio di un altro Stato, il paragrafo 3 dispone che ciascuno Stato richiesto abbia la capacità giuridica di ottenere la rapida conservazione dei dati archiviati nel territorio, al fine di neutralizzare il pericolo di alterazione, rimozione o cancellazione di essi durante il segmento temporale necessario per predisporre, trasmettere ed eseguire una richiesta di mutua assistenza per l'ottenimento dei dati.

Si tratta di una misura limitata e provvisoria – più rapida ed al tempo stesso meno invasiva – destinata ad ottenere effetti più celeri rispetto a quelli conseguibili con i tradizionali modelli di mutua assistenza, in risposta alle particolari caratteristiche intrinseche dell'elemento informatico⁶⁶⁸. Pertanto, si è convenuto di sviluppare una "tecnica di congelamento" quale risposta pressoché immediata per garantire la disponibilità dei dati in attesa del più lungo e complesso procedimento di esecuzione di una formale richiesta di assistenza reciproca.

Tale metodo non consente ai funzionari dell'assistenza giudiziaria della Parte richiesta di ottenere il possesso dei dati dal custode⁶⁶⁹, ma permette di assicurare che quest'ultimo conservi e non cancelli i dati in attesa dell'attivazione e dell'esecuzione delle procedure di assistenza giudiziaria volte alla raccolta dei dati. Questa procedura ha il vantaggio di essere rapida e al tempo stesso protettiva della tutela della privacy della persona a cui si riferiscono i dati, poiché questi non sono divulgabili o esaminabili da alcun funzionario pubblico fino a quando non saranno stati soddisfatti i criteri per la piena divulgazione ai sensi dei normali regimi di assistenza reciproca. Allo stesso tempo, una Parte richiesta è autorizzata a utilizzare altre procedure per garantire la rapida conservazione dei dati, compresa l'emissione e l'esecuzione accelerate di un ordine di produzione o un mandato di perquisizione per i dati⁶⁷⁰. Il requisito fondamentale è disporre di un processo estremamente rapido per evitare che i dati vengano irrimediabilmente persi.

Siccome trattasi di misura provvisoria e da eseguire in tempi celeri, il contenuto della richiesta è particolarmente semplificato, così da consentire una rapida preparazione e

International Cybercrime Treaty, cit., p. 274 ss.; D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, cit., p. 168.

⁶⁶⁶ In tal senso, F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 185.

⁶⁶⁷ Cfr., art. 29, par. 7, della Convenzione sulla criminalità informatica.

⁶⁶⁸ Con poche sequenze di tasti, o tramite il funzionamento di programmi automatici, può essere cancellato, modificato o spostato, rendendo impossibile risalire a un crimine al suo autore o distruggendo la prova critica di colpevolezza. Alcune forme di dati informatici vengono archiviate solo per brevi periodi di tempo prima di essere cancellate.

⁶⁶⁹ Il custode spesso è, all'evidenza, un *Internet Service Provider* o un'altra Parte terza.

⁶⁷⁰ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 283, p. 51.

trasmissione⁶⁷¹. Le informazioni richieste devono essere sintetiche e comprendono soltanto indicazioni minime necessarie per consentire la conservazione dei dati⁶⁷².

Siccome risulta controproducente, la regola generale vuole che non sia richiesta l'applicazione della condizione della doppia incriminazione, tendenza riscontrabile anche per le altre misure procedurali non così intrusive come la perquisizione, il sequestro o l'intercettazione.

Invero, la tecnica di conservazione del dato non risulta particolarmente invadente, perché si limita a "congelare" l'informazione digitale conservata dallo stesso custode che ne ha legalmente il possesso, evitando la divulgazione o l'esame da parte delle autorità dello Stato richiesto, se non dopo l'esecuzione della formale richiesta di mutua assistenza della comunicazione dei dati.

L'esclusione del principio della doppia incriminazione consente una notevole compressione dei tempi di esecuzione della procedura, poiché elimina l'intera fase dei chiarimenti e della valutazione necessari per stabilire l'esistenza della doppia incriminazione, limitando di fatto la possibilità di cancellazione, rimozione o modificazione dei dati informatici⁶⁷³.

Tuttavia, il paragrafo 4 prevede una riserva limitata di condizione della doppia incriminazione. La Parte richiesta può riservarsi il diritto di rifiutare la richiesta di *data freezing* nei casi in cui ha ragione di ritenere che, al momento della divulgazione, non sarà soddisfatta la doppia incriminazione, nelle ipotesi in cui questa sia condizione di procedibilità per rispondere ad una richiesta di mutua assistenza per una perquisizione o altro mezzo simile di accesso, un sequestro o altro strumento simile. Inoltre, la doppia incriminazione si presume *iuris et de iure* per i reati indicati dagli articoli da 2 a 11 della Convenzione⁶⁷⁴ sulla criminalità informatica, fatte salve le riserve che possono essere state formulate su tali reati, ove consentito dalla Convenzione.

⁶⁷¹ Il 9 luglio 2018, nel corso della diciannovesima plenaria, il T-CY ha adottato ed emanato il modulo di richiesta che gli Stati possono compilare al fine di richiedere la conservazione rapida dei dati informatici, ai sensi dell'art. 29, o la divulgazione rapida dei dati di traffico conservati, ai sensi dell'art. 30 della Convenzione sulla criminalità informatica. Il modulo è disponibile al link: <https://rm.coe.int/template-article29-request/1680a273d6>.

⁶⁷² L'art. 29, par. 2, della Convenzione sulla criminalità informatica specifica che la richiesta deve contenere l'autorità che richiede la conservazione; il reato che costituisce oggetto di indagine e una breve esposizione dei fatti relativi; l'indicazione dei dati informatici immagazzinati da conservare e il loro legame con il reato; tutte le informazioni utili ad identificare il custode dei dati informatici immagazzinati o il luogo dove si trova il sistema informatico; la necessità della conservazione; l'espressa esternazione della volontà della Parte richiedente di avanzare una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o uno strumento simile, o per la divulgazione dei dati. Per necessità della conservazione dei dati dovrebbe intendersi l'esigenza sottesa alla richiesta di conservazione, mentre la volontà della parte richiedente di avanzare una richiesta di mutua assistenza rappresenterebbe uno dei presupposti.

⁶⁷³ Ad esempio, nelle prime fasi di un'indagine, la Parte richiedente potrebbe essere a conoscenza di un'intrusione in un computer nel suo territorio, ma solo successivamente potrebbe avere una buona comprensione della natura e dell'entità del danno. Se la Parte richiesta ritardasse la conservazione dei dati utili per l'individuazione della fonte dell'intrusione in attesa dell'accertamento definitivo della doppia incriminazione, i dati critici verrebbero spesso eliminati di *routine* dai fornitori di servizi che li conservano in tempi ristretti. Anche se in seguito la parte richiedente fosse in grado di stabilire la doppia incriminazione, i dati cruciali sul traffico non potrebbero essere recuperati e l'autore del reato non sarebbe mai identificato. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 285, p. 51.

⁶⁷⁴ Si tratta dell'accesso illegale ad un sistema informatico (art. 2); dell'intercettazione abusiva (art. 3); dell'attentato all'integrità dei dati (art. 4); dell'attentato all'integrità di un sistema (art. 5); dell'abuso di apparecchiature (art. 6); della falsificazione informatica (art. 7); della frode informatica (art. 8); dei reati

Di conseguenza anche per l'applicazione del *data freezing* il principio della doppia incriminazione di fatto sembrerebbe previsto.

Limitati anche i motivi di rifiuto⁶⁷⁵. La richiesta di congelamento dei dati può essere rifiutata solo laddove la sua esecuzione pregiudichi la sovranità, la sicurezza, l'ordine pubblico o altri interessi essenziali, o laddove lo Stato di esecuzione consideri il reato un reato politico o un reato connesso con un reato politico⁶⁷⁶.

L'articolo non rinvia ai motivi di rifiuto contenuti all'art. 25, par. 4, della Convenzione sulla criminalità informatica, come invece previsto dall'art. 27, par. 4. Pertanto, deve ritenersi che non sia possibile estendere tali motivi al *data freezing*⁶⁷⁷. Se avesse voluto

relativi alla pornografia infantile (art. 9); dei reati contro la proprietà intellettuale e diritti collegati (art. 10). In tutti i casi si considerano anche le forme del tentativo e nei casi di concorso (art. 11).

⁶⁷⁵ Sul punto, B. ISENRING, R.D. MAYBUD, L. QUIBLIER, *Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick*, in *Schweizerische Juristen-Zeitung*, 2019, p. 445; C. SCHWARZENEGGER, *Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 – Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses*, in AA.VV., *Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag* (eds. A. DONATSCH, M. FORSTER, C. SCHWARZENEGGER), Zürich, 2002, p. 310; L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, cit., p. 1209; D. WICKI-BIRCHLER, *The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?*, cit., p. 68.

⁶⁷⁶ Cfr., art. 29, par. 5, lett. a) e b) della Convenzione sulla criminalità informatica.

⁶⁷⁷ Come già si è avuto modo di sottolineare, l'art. 25, par. 4 della Convenzione sulla criminalità informatica stabilisce la regola generale secondo cui l'assistenza reciproca è soggetta alle condizioni e ai motivi di rifiuto posti dalla legge della Parte richiasta o dai trattati di mutua assistenza applicabili. Pertanto, in base a questa disposizione una Parte potrebbe decidere di stabilire dei motivi di rifiuto relativi alla *data protection* nelle ipotesi di trasferimento di dati tra autorità straniere. L'assenza di rinvio a tale articolo da parte dell'articolo 29 sembrerebbe bloccare la possibilità di rifiutare una richiesta relativa a un procedimento in contrasto con la disciplina interna alla *data protection*. Tuttavia, parte della dottrina ritiene che la protezione dei dati potrebbe rientrare nella categoria dell'"ordine pubblico" o in quella degli "altri interessi essenziali". In particolare, si osserva che il concetto di ordine pubblico non è di matrice internazionale, ma di diritto interno. L'ordine pubblico abbraccia un insieme di principi e di valori fondamentali alla base dello Stato di diritto, riferendosi specificamente ai diritti umani. Ad esempio, l'art. 6 dell'*Einführungsgesetz zum Bürgerlichen Gesetzbuche* (EGBGB) afferma che il concetto di ordine pubblico rinvia ai principi fondamentali del diritto tedesco, e in particolare ai diritti umani. Anche la tutela della dignità umana è spesso menzionata come uno dei valori fondamentali riferibili all'ordine pubblico. Ad esempio, la direttiva 2000/31/CE sul commercio elettronico afferma che la prevenzione e il perseguimento delle violazioni della dignità umana della persona rientrano nei motivi di ordine pubblico che possono giustificare deroghe nazionali alle norme che essa stabilisce. Anche fuori dai confini europei la dignità umana è considerata alla base del diritto alla privacy. Nello specifico, la Corte Suprema indiana, con la sentenza *Justice K S Puttaswamy (Retd) and Anr. vs. Union of India and Ors.* (decisione del 24 agosto 2017), 262, ha riconosciuto che la privacy è il nucleo costituzionale della dignità umana. Sulla base di ciò, c'è chi ritiene che uno Stato possa invocare la tutela del proprio ordine pubblico come motivo di rifiuto della cooperazione in procedimenti che potrebbero comportare una grave violazione del diritto alla privacy.

La privacy può anche rientrare nella categoria degli "interessi essenziali". Infatti, la relazione esplicativa alla Convenzione sulla criminalità informatica afferma che il rifiuto dell'assistenza per motivi di protezione dei dati può essere invocato se, bilanciando gli interessi fondamentali coinvolti nel caso specifico (da un lato, interessi pubblici, compresa la buona amministrazione della giustizia e, dall'altro, gli interessi relativi alla privacy), dopo aver fornito i dati specifici richiesti dalla Parte richiedente, sollevasse difficoltà così rilevanti da essere considerata dalla Parte richiasta come riconducibile all'interesse essenziale. Sul punto, M. GEBAUER, F. BERNER, *Ordre Public (Public Policy)*, in *Max Planck Encyclopedias of International Law*, agosto 2019, disponibile al link: <https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1448?rskey=x5B2W2&result=1&prd=EPIL>; L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, cit., p. 1209.

operare un'estensione in tal senso, si sarebbe proceduto a rinvio esplicito, così come previsto per l'art. 27.

Invero, l'assoluta centralità della misura per l'effettività delle indagini e per l'efficace lotta ai reati informatici ha consentito alle Parti contraenti di convergere verso una preclusione rispetto all'affermazione di qualsiasi altro motivo di rifiuto della richiesta di conservazione dei dati.

Particolarmente interessante risulta la previsione al paragrafo 6. Ivi, si impone l'obbligo di confronto tra Parti, al fine di decidere se eseguire la richiesta nonostante la Parte «ritenga che la conservazione non assicurerà la disponibilità in futuro dei dati o comprometterà la confidenzialità o pregiudicherà in altro modo le indagini della Parte richiedente».

Si tratta di particolari ipotesi in cui la Parte richiesta ritiene probabile che il custode dei dati tenga una condotta tale da compromettere la riservatezza o arrecare pregiudizio alle indagini della Parte richiedente⁶⁷⁸. In tali situazioni, il confronto tra Parti consente di valutare se sia più proficuo assumersi il rischio posto dall'esecuzione della richiesta di conservazione ovvero cercare una forma di mutua assistenza più invasiva, ma che assicuri un risultato costruttivo per le indagini come una richiesta di produzione o di ricerca o di sequestro⁶⁷⁹.

È possibile che, nel corso dell'esecuzione di una richiesta di *data freezing*, la Parte richiesta scopra il coinvolgimento nella trasmissione della comunicazione di un *service provider* di un altro Stato. In tali ipotesi, l'art. 30 della Convenzione sulla criminalità informatica⁶⁸⁰ pone l'obbligo in capo alla Parte richiesta di trasmettere rapidamente alla

⁶⁷⁸ Ad esempio, casi in cui i dati da conservare sono detenuti da un fornitore di servizi controllato da un gruppo criminale, o dallo stesso destinatario dell'indagine.

⁶⁷⁹ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 288, p. 52.

⁶⁸⁰ L'articolo è l'equivalente internazionale del potere stabilito per l'uso interno dall'art. 17 della Convenzione sulla criminalità informatica. L'art. 17 della Convenzione sulla criminalità informatica disciplina la conservazione e divulgazione rapide di dati relativi al traffico. Ai sensi dell'art. 17 della Convenzione sulla criminalità informatica, «1. Al fine di assicurare la conservazione dei dati relativi al traffico in applicazione di quanto previsto all'articolo 16 ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per: a. assicurare che la conservazione dei dati relativi al traffico sia disponibile nonostante uno o più fornitori di servizi siano stati coinvolti nella trasmissione di tale comunicazione; e b. assicurare la rapida trasmissione all'autorità competente della Parte, o al soggetto designato da tale autorità, di una quantità di dati relativi al traffico sufficiente per consentire alla Parte di identificare il fornitore di servizi e la via attraverso la quale la comunicazione fu trasmessa.

2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15».

In Italia, l'art. 17 è stato recepito con l. 18 marzo 2008, n. 48, la quale, con l'art. 9 è intervenuta sull'art. 132, d. lgs. 30 giugno 2003, n. 196 (in G.U. 29 luglio 2003, n. 174, suppl. ord. n. 123) rubricato "Conservazione di dati di traffico per altre finalità". La norma consente la *data retention*, ossia l'acquisizione presso i fornitori di servizi telefonici o telematici di una serie di dati esterni generati da ogni comunicazione e che possono acquisire un valore investigativo nei procedimenti penali, e nel tempo ha conosciuto sette versioni prima di quella vigente. Attualmente, per l'istituto della *data retention* è previsto un doppio binario: da una parte vi è la previsione dell'art. 132, d. lgs. 30 giugno 2003, n. 196, per i reati comuni; dall'altra l'art. 24, l. 20 novembre 2017, n. 167 (in G.U. 27 novembre 2017, n. 277) regola l'istituto per i reati di crescente allarme sociale, individuati agli artt. 51, comma 3-*quater* e 407, comma 2, lett. a) c.p.p. Recentemente, con d.l. 30 settembre 2021, n. 132 (in G.U. 30 settembre 2021, n. 234), convertito, con modificazioni, in l. 23 novembre 2021, n. 178 (in G.U. 29 novembre 2021, n. 284), l'art. 132, d. lgs. n. 196/2003 ha subito una modifica, ritenuta necessaria a seguito della sentenza della Corte di giustizia dell'Unione europea, Grande sezione, 2 marzo 2021, causa C-746/18, *H.K.*, per garantire la possibilità di acquisire dati relativi al traffico telefonico e telematico per fini di indagine penale nel rispetto della sentenza indicata, la quale ha espresso la necessità di circoscrivere le attività di acquisizione ai procedimenti penali aventi ad oggetto forme gravi di criminalità e di garantire che dette attività siano soggette al controllo di un'autorità giurisdizionale.

Attualmente, l'art. 132, d. lgs. n. 196/2003 stabilisce che «1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione.

1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni.

2. Abrogato

3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private.

3-bis. Quando ricorrono ragioni di urgenza e vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che è comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato.

3-ter. Rispetto ai dati conservati per le finalità indicate al comma 1 i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalità di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.

3-quater. I dati acquisiti in violazione delle disposizioni dei commi 3 e *3-bis* non possono essere utilizzati.

4. Abrogato

4-bis. Abrogato

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma *4-ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma *4-ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

5. Abrogato

5-bis. È fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167».

Invece, per quanto attiene ai reati di maggior allarme sociale, l'art. 24, l. 167/2017 recita: «In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15.3.2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del

terrorismo, anche internazionale, per le finalità di accertamento e della repressione dei reati di cui agli articoli 51, comma 3-*quater*, e 407, comma 2, lettera a, del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'articolo 4-*bis*, commi 1 e 2, del decreto-legge 18.2.2015, n. 7, convertito, con modificazioni, dalla legge 17.4.2015, n. 43, è stabilito in settantadue mesi, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-*bis*, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30.6.2003, n. 196».

L'istituto della *data retention* non va confuso con il sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni di cui all'art. 254-*bis* c.p.p., inserito dall'art. 7, comma 5, d. lgs. 48/2008, in recepimento dell'art. 19 della Convenzione sulla criminalità informatica, relativo alla perquisizione ed al sequestro dei dati informatici immagazzinati.

Per un'analisi critica della disciplina sulla *data retention*, S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1579 ss. V., inoltre, E. ANDOLINA, *La raccolta dei dati relativi alla localizzazione del cellulare ed al traffico telefonico tra inerzia legislativa e supplenza giurisprudenziale*, in *Arch. Pen.*, 3, 2020, p. 1 ss.; ID., *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018, *passim*; ID., *Il potere del difensore di acquisizione diretta dei dati di traffico telefonico relativi al proprio assistito: limiti normativi e prospettive "de iure condendo"*, in *Arch. nuova proc. pen.*, 1, 2018, p. 1 ss.; P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Arch. pen.*, 1, 2016, p. 28 ss.; C. CONTI, *L'acquisizione dei tabulati (c.d. data retention)*, in P. TONINI, C. CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 470 ss.; F. FALATO, *L'uso (preventivo e repressivo) dei dati personali come compressione di un diritto inviolabile*, in *Giust. pen.*, 10, 2016, p. 548 ss.; R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata questio (?)*, in *penalecontemporaneo.it*, 29 marzo 2017; B. GALGANI, *Giudizio penale, habeas data, e garanzie fondamentali*, in *Arch. pen.*, 1, 2019, p. 1 ss.; F. IOVENE, *"Data retention" tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 12, 2014, p. 4274 ss.; V. MANES, F. MAZZACUVA, *GDPR e nuove disposizioni penali del codice privacy*, in *Dir. pen. e proc.*, 2, 2019, p. 171 ss.; M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., p. 52 ss. e 122 ss.; M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico – Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Dir. pen. cont.*, 3, 2016, p. 157 ss.; F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.*, 6, 2017, p. 2483 ss.; V. VASTA, *Tracciamento elettronico e tabulati telefonici: anche l'Italia a rischio condanna?*, in *Riv. it. dir. e proc. pen.*, 2, 2018, p. 985 ss.

Sulla recente riforma dell'istituto, F. CRIMI, *D.L. n. 132/2021: per l'acquisizione dei tabulati telefonici servirà l'autorizzazione del g.i.p.*, in *Quotidiano giuridico*, 5 novembre 2021; L. FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *Penale Diritto e Procedura*, 1 ottobre 2021, p. 1 ss., disponibile al link: <https://penaledp.it/la-nuova-disciplina-dei-tabulati-il-commento-a-caldo-del-prof-filippi/>; C. GITTARDI, *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *Giustizia insieme*, 7 ottobre 2021, p. 1 ss., disponibile al link: <https://www.giustiziainsieme.it/it/processo-penale/1975-sull-utilizzabilita-dei-dati-del-traffico-telefonico-e-telematico-acquisiti-nell-ambito-dei-procedimenti-pendenti-alla-data-del-30-settembre-2021>; A. MALACARNE, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi principi in materia di data retention*, in *Riv. It. Dir. e proc. pen.*, 3, 2021, p. 1164 ss.; ID., *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *Sistema penale*, 8 ottobre 2021, p. 1 ss., disponibile al link: <https://www.sistemapenale.it/it/scheda/decreto-legge-132-2021-tabulati-telefonici-malacarne-commento-a-prima-lettura>; W. NOCERINO, *La nuova (e incompleta) disciplina dei tabulati telefonici in Italia*, in *Intelligence Security Investigation*, 30 novembre 2021, p. 1 ss., disponibile al link: <https://intelligencesecurityinvestigation.it/la-nuova-e-incompleta-disciplina-dei-tabulati-telefonici-in-italia/>; G. PESTELLI, *D.L. 132/2021: un indiscutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *Quotidiano giuridico*, 4 ottobre 2021.

Per un'analisi critica della giurisprudenza internazionale ed europea in tema di *data retention*, M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il diritto dell'Unione europea*, 1, 2021, p. 93 ss.

Parte richiedente una quantità sufficiente di dati relativi al traffico che consenta di identificare il *service provider* e la via attraverso la quale la comunicazione fu effettuata, sì da consentire l'inoltro di un'ulteriore richiesta di assistenza giudiziaria⁶⁸¹.

Ed invero, accade spesso che uno Stato richiesto si riveli un “luogo di passaggio”, nel tortuoso viaggio affrontato dai dati. In tal caso, la Parte richiesta conserva i dati sul traffico relativi a una trasmissione che ha viaggiato attraverso i suoi *server*, al fine di risalire alla fonte della trasmissione e identificare l'autore del reato o individuare ulteriori elementi di prova. Attraverso la conservazione dei dati, la Parte richiesta può scoprire se i dati sul traffico trovati nel suo territorio rivelano che la trasmissione era stata instradata da un fornitore di servizi in uno Stato terzo o da un fornitore nello Stato richiedente stesso.

La comunicazione di essi è di enorme valore, perché consentirà alla Parte richiedente di continuare proficuamente nelle indagini, sino a risalire alla sua fonte ultima. Tuttavia, va osservato come la procedura sia particolarmente onerosa sia da un punto di vista economico, sia da un punto di vista temporale.

Simile meccanismo comporta l'emissione in sequenza di molteplici richieste di mutua assistenza, l'una successiva all'altra, sino all'identificazione della fonte ultima. Siccome la pratica della migrazione dei dati attraverso vari *server* è particolarmente diffusa, le autorità sono scoraggiate e, a causa dei costi elevati, dei tempi troppo lunghi e delle ulteriori difficoltà nell'ottenimento delle informazioni, spesso non riescono ad assicurare gli elementi idonei a sostenere l'accusa in giudizio. Conseguenza è l'assenza di una risposta positiva e soddisfacente nei confronti del cittadino comune, utente ultimo della macchina della giustizia.

Come per l'art. 29, la divulgazione dei dati di traffico può essere rifiutata solo in casi limitati: se la Parte richiesta consideri che il reato per cui si è attivata la procedura sia un reato politico o connesso a reato politico ovvero se ritenga che l'esecuzione della richiesta possa recare pregiudizio alla sovranità, alla sicurezza, all'ordine pubblico o ad altri interessi essenziali dello Stato.

Un secondo gruppo di norme regola le attività d'indagine. Sono specifiche attività d'indagine: la perquisizione, il sequestro o ogni altra attività simile volta all'apprensione del dato digitale (art. 31); l'accesso diretto ai dati immagazzinati in un sistema informatico situato all'estero (art. 32); la raccolta in tempo reale dei dati relativi al traffico (art. 33); l'intercettazione di dati relativi al contenuto (art. 34).

L'art. 31⁶⁸², rubricato “mutua assistenza concernente l'accesso a dati informatici immagazzinati”, autorizza una parte a richiedere assistenza reciproca per la perquisizione

⁶⁸¹ Sul tema, E. SELVAGGI, *Task force operativa 24 ore al giorno*, cit., p. 74.

⁶⁸² L'articolo è lo speculare internazionale dell'art. 19 della Convenzione sulla criminalità informatica, formulato per scopi domestici e rubricato ricerca e sequestro dei dati informatici. Ai sensi dell'art. 19, rubricato “perquisizione e sequestro dei dati informatici immagazzinati” «1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di perquisire o accedere in modo simile: a. a un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati; e b. a supporto per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati nel proprio territorio.

2. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire che, qualora le proprie autorità perquisiscano o accedano in modo simile a specifici sistemi informatici o parte di essi, in conformità al paragrafo 1.a, e abbiano ragione di ritenere che i dati ricercati si trovino presso un altro sistema informatico o parte di esso nel proprio territorio, e a tali dati sia possibile legalmente l'accesso dal sistema iniziale, le stesse autorità possano estendere rapidamente la perquisizione o l'accesso all'altro sistema.

3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i

o mezzo simile, il sequestro o strumento simile, e la divulgazione dei dati immagazzinati in un sistema informatico collocato sul territorio di uno Stato estero⁶⁸³. La richiesta può avere ad oggetto sia dati congelati con lo strumento del *data freezing* di cui all'art. 29, sia di dati che non siano stati preventivamente conservati⁶⁸⁴.

Mentre il par. 1 attribuisce un potere in capo alla Parte richiedente, il par. 2 pretende dalla Parte richiedente la capacità di fornire assistenza attraverso gli strumenti internazionali sulla cooperazione internazionale in materia penale, gli accordi e le legislazioni, e in conformità alle disposizioni contenute nel capitolo III sulla cooperazione internazionale della Convenzione sulla criminalità informatica⁶⁸⁵.

La dottrina⁶⁸⁶ ritiene che tale previsione sembri imporre un'intrusione veicolata attraverso i tradizionali meccanismi di cooperazione giudiziaria, ogni volta che risulti nota la sede del sistema informatico, anche utilizzando moderni sistemi di accesso quali, ad esempio, il captatore informatico⁶⁸⁷.

quali si è proceduto all'accesso in conformità ai paragrafi 1 o 2. Tali misure devono includere il potere di: a. sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici; b. fare e trattenere una copia di quei dati informatici; c. mantenere l'integrità dei relativi dati informatici immagazzinati; d. rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato.

4. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie per consentire l'applicazione delle misure di cui ai paragrafi 1. e 2.

5. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15».

L'Italia si è adeguata a quanto stabilito dall'art. 19 con l'art. 7, d. lgs. 48/2008, il quale ha inserito il nuovo art. 254-bis c.p.p. Quest'ultimo, rubricato "sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni" recita: «1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali». In dottrina, R.M.F. BARON, *A Critique of the International Cybercrime Treaty*, cit., p. 276 ss.; D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, cit., p. 169; J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 710 ss.; M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 313 ss.; M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, cit., p. 342 ss.

⁶⁸³ Cfr., M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 320.

⁶⁸⁴ Il 9 luglio 2018, nel corso della diciannovesima plenaria, il T-CY ha adottato ed emanato il modulo di richiesta che gli Stati possono compilare al fine di richiedere, ai sensi dell'art. 31 della Convenzione sulla criminalità informatica, la mutua assistenza relativa all'accesso ai dati informatici immagazzinati. Il modulo è disponibile al link: <https://rm.coe.int/template-article31-mla-subscriber/1680a273d9>.

⁶⁸⁵ Invero, vige il principio secondo cui i termini e le condizioni per fornire tale cooperazione dovrebbero essere quelli stabiliti nei trattati, accordi e leggi nazionali applicabili che disciplinano l'assistenza giudiziaria in materia penale. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 292, p. 52.

⁶⁸⁶ Cfr., F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 185.

⁶⁸⁷ Sul captatore informatico, *ex multis*, A. MARANDOLA, *Sviluppo tecnologico e uso del c.d. captatore informatico*, in *Studium Iuris*, 11, 2017, p. 1285 ss.; W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021, *passim*; L. PALMIERI, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza "Scurato" alla riforma sulle intercettazioni*, in *Dir. pen. cont.*, 1, 2018, p. 59 ss.

Per rispondere ad una esigenza di celerità, alla richiesta deve essere data una risposta in tempi rapidi⁶⁸⁸ all'avveramento di due presupposti tra loro alternativi: in caso di urgenza, perché vi è il pericolo per l'acquisizione o la genuinità dei dati informatici; nel caso in cui esistano accordi o legislazioni che prevedono strumenti di cooperazione rapida.

Particolarmente singolare ed innovativa è la disciplina relativa all'accesso transfrontaliero ai dati informatici immagazzinati con il consenso o quando pubblicamente disponibili. L'art. 32 della Convenzione sulla criminalità informatica⁶⁸⁹ introduce un «modello di “nuovo” conio, stravagante rispetto ai tradizionali strumenti di cooperazione giudiziaria»⁶⁹⁰, poiché il procedimento evita il rapporto tra Stati e tra autorità straniere, a favore dell'apprensione diretta del dato collocato all'estero o di un diretto contatto con la persona legalmente autorizzata alla divulgazione dell'informazione⁶⁹¹.

Si tratta di un meccanismo simile all'ingiunzione di produrre (o ordine di produzione) previsto all'art. 18 della Convenzione sulla criminalità informatica⁶⁹², diversificandosene

⁶⁸⁸ L'art. 31, par. 3 afferma che l'esecuzione deve avvenire il «più presto possibile».

⁶⁸⁹ Sul tema, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 719 ss.; M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 320; E. SELVAGGI, *Task force operativa 24 ore al giorno*, cit., p. 74; G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, cit., p. 117 ss.; ID., *Il ruolo del consenso del sovrano territoriale nel transborder data access tra obblighi internazionali e norme interne di adattamento*, in *La Comunità internazionale*, 2, 2016, p. 198 ss. Per un'analisi dell'art. 32 della Convenzione sulla criminalità informatica si vedano la *Guidance Note # 3 on Transborder access to data (Article 32)*, T-CY (2013)7 E, del 19 febbraio 2013, nonché il rapporto *Transborder access to data and jurisdiction: Options for further action by the T-CY*, T-CY (2014)16, del 3 dicembre 2014, redatti dal CYBERCRIME CONVENTION COMMITTEE. Si veda, inoltre, il *discussion paper* del CLOUD EVIDENCE GROUP, *Criminal justice access to data in the cloud: challenges*, T-CY (2015)10, del 26 maggio 2015.

⁶⁹⁰ F. SIRACUSANO, *La prova informatica transnazionale: un difficile “connubio” fra innovazione e tradizione*, cit., p. 185.

⁶⁹¹ Si può ritenere che si tratta del primo strumento di cooperazione di “terzo tipo” per la formazione della prova transnazionale. Mentre il principio della mutua assistenza si basa sul modello della richiesta e del metodo intergovernativo, ed il mutuo riconoscimento sul rapporto diretto tra autorità giudiziarie; il nuovo strumento di cooperazione introduce il sistema del “consenso” del soggetto che può disporre legalmente del dato da acquisire. Similmente, accadrà con i nuovi ordini di produzione e di conservazione europei. Sul tema, anche, F. SIRACUSANO, *La prova informatica transnazionale: un difficile “connubio” fra innovazione e tradizione*, cit., p. 185.

⁶⁹² Si è ritenuto che oltre all'art. 32, anche l'art. 18 della Convenzione sulla criminalità informatica consenta alle forze dell'ordine l'accesso diretto ai dati archiviati in un'altra giurisdizione. Questa tesi è stata sostenuta dalla Corte Suprema statunitense, basandosi sul fatto che la disciplina richiede agli Stati di autorizzare le loro autorità a ordinare ad una persona sul proprio territorio o a un *internet service provider* che offre i propri servizi sul loro territorio di consegnare i dati in loro possesso o in loro controllo, senza specificare che i dati debbano trovarsi nel territorio dello Stato richiedente. V. *Brief for the United States, United States v. Microsoft Corporation*, No. 17-2, 6 dicembre 2017, p. 46 ss., disponibile al link: https://www.supremecourt.gov/DocketPDF/17/17-2/22902/20171206191900398_17-2tsUnitedStates.pdf.

Va però osservato che l'art. 18 della Convenzione sulla criminalità informatica non fa alcun riferimento esplicito ai dati conservati all'estero. Ciò suggerirebbe che l'ingiunzione di produrre copra solo i dati archiviati a livello nazionale. Tale tesi sembra essere confermata dal principio dell'efficacia nell'interpretazione dei trattati, secondo cui un interprete deve dare effetti a tutti i termini del trattato, evitando di adottare una lettura che comporti una riduzione di intere clausole o paragrafi del trattato, rendendoli inutili o ridondanti. Pertanto, l'art. 18, par. 1, lett. a) riguarderebbe gli ordini di produzione per situazioni meramente interne, mentre l'art. 32, lett. b) si applicherebbe a tutte le situazioni in cui la persona che acconsente a fornire l'accesso si trovi nel territorio della parte richiedente. V., anche, L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, cit., p. 1210. A quest'ultima

per taluni aspetti, e all'ordine europeo di produzione, allo studio del Consiglio e del Parlamento europeo.

Invero, con tale strumento uno Stato può accedere unilateralmente ai dati informatici immagazzinati in sistemi collocati all'estero senza attivare una procedura di mutua assistenza, con evidente risparmio di risorse economiche e in tempi ragionevoli⁶⁹³.

I redattori della Convenzione, all'epoca, ritennero che le circostanze non fossero ancora mature per approntare un procedimento completo e giuridicamente vincolante, che regolasse tale strumento⁶⁹⁴, pertanto preferirono enunciare soltanto le situazioni in cui vi fosse stato un consenso unanime sull'ammissibilità di esso⁶⁹⁵.

L'accesso ai dati collocati all'estero può avvenire attraverso un sistema presente sul proprio territorio, senza alcuna autorizzazione dello Stato estero, secondo due presupposti alternativi: i dati siano pubblicamente disponibili o che vi sia il consenso della persona fisica o giuridica legalmente autorizzata.

Per quanto attiene al primo presupposto, si ritiene che non siano disponibili al pubblico i dati informatici non condivisi pubblicamente con una pluralità di individui e non diffusi sulla rete, o tutti i dati mantenuti riservati, protetti o conservati nel *deep web*, ossia in aree accessibili solo mediante credenziali di autenticazione o con chiavi basate su un sistema crittografico, ovvero le informazioni condivise solo con un gruppo ristretto di utenti⁶⁹⁶.

tesi, in dottrina, se ne contrappone una che ammette l'emissione di ingiunzione di produrre anche per dati archiviati all'estero (v., *infra*, par. 5).

⁶⁹³ Nel 2009-2010, il T-CY ha svolto un'indagine sull'accesso transfrontaliero diretto ai dati e ai flussi di dati. Le risposte suggeriscono che le autorità di contrasto di molti Stati effettuano ricerche transfrontaliere, ma che le condizioni e le pratiche differiscono. Per i risultati dello studio, TRANSBORDER GROUP, *Transborder Access and Jurisdiction: What Are the Options?*, Discussion Paper No T-CY(2012)3, Cybercrime Convention Committee, Council of Europe, 6 dicembre 2012, p. 29 ss.

⁶⁹⁴ Sul punto, E. SELVAGGI, *Task force operativa 24 ore al giorno*, cit., p. 74. V., inoltre, A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione Europea sugli ordini di produzione e conservazione di prove elettroniche (E-Evidence)*, in *La Legislazione penale*, 16 ottobre 2020, p. 4.

⁶⁹⁵ Le difficoltà erano dettate sia dall'assenza di esperienze concrete con tali situazioni, sia alla consapevolezza che la soluzione più adeguata spesso dipendeva da precise circostanze del singolo caso, rendendo difficile la formulazione di regole generali. Pertanto, i redattori della convenzione hanno convenuto di non regolare ulteriori situazioni fino a quando non sarà possibile avviare una nuova discussione con il possesso di ulteriori dati empirici. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 293, p. 53. V., in dottrina, F. GRAZIANI, *L'acquisizione della prova digitale all'estero: verso un secondo Protocollo addizionale alla Convenzione di Budapest sul cybercrime*, cit., p. 62, secondo cui si tratterebbe di un «testo compromissorio e ambiguo».

⁶⁹⁶ Così, S. ATERNO, *L'acquisizione dei dati personali tra misure antiterrorismo e intromissioni nella privacy*, in *Arch. pen.*, 1, 2016, p. 165; F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 185. Altra parte della dottrina, in parziale contrapposizione, ha chiarito che a fini investigativi, non sembra rilevare tanto il carattere riservato dell'informazione, quanto il carattere riservato del luogo della rete in cui l'informazione è contenuta. Infatti, un'informazione che potrebbe essere riservata, se posta in un luogo pubblicamente accessibile, sfuggirebbe alla tutela della *privacy*; viceversa, un'informazione non riservata, se posta in un luogo che rientra nella sfera di tutela della *privacy*, potrebbe essere visualizzata ed acquisita a fini investigativi solo nel rispetto del diritto alla *privacy*. Diventa, dunque, fondamentale la caratteristica assunta dal luogo in cui è allocato il dato. Se si tratta di un luogo accessibile a chiunque, si è in presenza di un luogo pubblico. In tale spazio della rete è possibile accedere senza registrazioni e le informazioni sono visualizzabili da tutti; pertanto, potranno essere visionate ed acquisite a fini investigativi, senza limitazioni e – di conseguenza – con i sistemi previsti dall'art. 32, par. 1, lett. a., della Convenzione. Nei luoghi aperti al pubblico può accedere chiunque si renda riconoscibile o nel rispetto di determinate regole. Nel web, si accede in tali luoghi a condizione di essere registrati o di aver fornito la propria identità. Secondo tale dottrina – divergendo da

Nell'ipotesi di dati pubblicamente disponibili, le autorità investigative possono scaricare dati, acquisire schermate o, allo stesso modo, proteggere tali dati e utilizzarli come elementi di prova in procedimenti penali, senza la necessità di alcuna forma di assistenza giudiziaria né autorizzazione dello Stato in cui si trova il sistema informatico che ospita il sistema informatico in cui il dato è immagazzinato⁶⁹⁷.

Secondo presupposto è l'acquisizione preventiva del consenso «legale e volontario» della persona legalmente autorizzata a divulgare i dati allo Stato attraverso il sistema informatico. Per consenso legale dovrebbe intendersi un consenso ottenuto nel rispetto del principio di legalità, lecito, in conformità ai valori della Costituzione⁶⁹⁸.

Il consenso volontario sembrerebbe rinviare ad un'autorizzazione espressa, ottenuta con un'azione scevra da costrizioni e coercizioni fisiche o psicologiche, artifizii o raggiri, e frutto della libera autodeterminazione della persona. Anche il consenso dato da minori o persone incapaci di agire non sembrerebbe essere sufficiente, fatto salvo diversa disposizione del diritto interno.

Il «criterio» del consenso sottrae il tema della ricerca e formazione della prova al classico principio di territorialità per ancorarlo alla manifestazione di volontà del titolare del dato. Evidente il risvolto pratico: si consente alle autorità e forze dell'ordine di un Paese di condurre un'indagine extraterritoriale in un altro Paese, senza avvisare le autorità di quel Paese⁶⁹⁹.

quanto descritto in precedenza – si sfugge alla regola della *privacy*, poiché la persona che inserisce i propri dati cede volontariamente delle informazioni ad altre persone che non conosce, anche se facenti parte di un gruppo ristretto. Pertanto, anche le attività investigative potrebbero essere condotte senza alcun provvedimento dell'autorità pubblica, e quindi anche secondo le tecniche di cui all'art. 32 della Convenzione sulla criminalità informatica. Infine, gli spazi virtuali che non integrano un domicilio digitale si caratterizzano per un'aspettativa di riservatezza. In tali ipotesi le attività investigative devono sottostare alle regole poste a tutela della *privacy*. In questa categoria non sarebbero ricompresi anche i luoghi digitali riservati come quelli accessibili in forza di una selettiva accettazione dal gestore del luogo. In tali spazi, una volta ottenuta l'autorizzazione, l'attività investigativa potrebbe essere compiuta senza applicare le regole restrittive a presidio della *privacy*, avendo il gestore acconsentito all'ingresso di altri nel proprio luogo digitale riservato. In tale ultimo caso sembrerebbe applicabile la disciplina dell'art. 32 della Convenzione sulla criminalità informatica. Sul punto, S. SIGNORATO, *Le indagini digitali*, cit., p. 79 ss.

⁶⁹⁷ Si ritiene che l'accesso a dati pubblicamente disponibili per scopi di giustizia penale sia una pratica internazionale accettata e, quindi, parte del diritto consuetudinario internazionale a causa dell'uso generalizzato e mondiale di Internet, dell'ignoranza da parte degli utenti del luogo fisico in cui i dati sono immagazzinati e per la bassa intensità dell'intrusione nell'accedere ai dati pubblici nel cyberspazio. Sul punto, N. SEITZ, *Transborder Search: A new perspective in law enforcement?*, in *International Journal of Communications Law & Policy*, 9 – Special Issue in Cybercrime, 2004, p. 9 ss.; U. SIEBER, *Straftaten und Strafverfolgung im Internet: Gutachten C zum 69. Deutschen Juristentag*, München, 2012, p. 144 ss. Per parte della dottrina, vi sono, però, crescenti incertezze sulla legalità delle modalità di raccolta ed uso di tali dati. Cfr., A. LYLE, *Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism*, in AA.VV., *Open Source Intelligence Investigation: from Strategy to Implementation* (B. AKHGAR, P. S. BAYERL, F. SAMPSON eds.), Heidelberg, 2017, p. 281; M. O'FLOINN, D. ORMEROD, *Social networking sites, RIPA and criminal investigations*, in *Criminal Law Review*, 10, 2011, p. 766 ss.; M. O'FLOINN, D. ORMEROD, *Social networking materials as criminal evidence*, in *Criminal Law Review*, 7, 2012, p. 486 ss.; A. SAGLIOCCA, *Open Source Intelligence e Deep Web: Scenari Moderni delle Investigazioni Digitali*, in *Cyberspazio e diritto*, 1, 2017, p. 171 ss.

⁶⁹⁸ Sul concetto di legalità, P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, cit., p. 290.

⁶⁹⁹ Ad esempio, il proprietario di un *account* di posta elettronica i cui i dati sono stati archiviati in un *server* posto in un altro Paese può scegliere di divulgare volontariamente o consentire l'accesso a tali dati alla polizia giudiziaria locale. Il potenziale impatto della disposizione è evidente se si considera che gran parte delle moderne reti di comunicazione e la memorizzazione dei dati associati è di proprietà privata: si

Ci si interroga su chi sia la «persona legalmente autorizzata» alla divulgazione dei dati informatici. Nel silenzio della Convenzione, deve ritenersi che sia necessaria una valutazione in concreto delle circostanze, della natura della persona e della legge applicabile⁷⁰⁰. È chiaro però che la persona non solo deve avere il legittimo potere di divulgare i dati, ma tale divulgazione deve essere essa stessa lecita. Pertanto, spetterebbe ai singoli Stati determinare la misura in cui i propri cittadini possono divulgare legalmente i dati⁷⁰¹.

A causa della fumosità con cui è formulata la norma, la dottrina si divide. Alcuni ritengono che un fornitore di servizi disponga di tale legittima autorità se si riserva il diritto di divulgare i dati dei clienti alle autorità preposte all'applicazione della legge attraverso l'accordo contrattuale che stipula con i suoi clienti⁷⁰². Altri pensano che la sottoscrizione dell'accordo generale da parte di una persona sui termini e le condizioni di un servizio *online* utilizzato non costituirebbe consenso esplicito anche se questi termini e condizioni indicano che i dati possono essere condivisi con le autorità giudiziarie in caso di violazioni⁷⁰³.

Nel tentativo di trovare una soluzione nel rispetto del principio di ragionevolezza e proporzionalità, nel bilanciare gli interessi alla repressione del crimine e il diritto alla riservatezza imposto dal Preambolo della Convenzione, gli Stati hanno convenuto con una nota di orientamento – dunque, non giuridicamente vincolante – che gli *internet service provider* non hanno il potere di acconsentire validamente e volontariamente alla divulgazione dei dati dei propri utenti ai sensi dell'art. 32, essendone solo i titolari e non disponendo del controllo e del possesso di questi⁷⁰⁴, con la conseguenza che l'applicazione pratica dell'art. 32, lett. b) sia da limitare solo ai casi in cui il proprietario dell'*account* dia il consenso libero e volontario.

Un simile strumento potrebbe creare dubbi sul rispetto dei diritti fondamentali da parte degli Stati che acquisirebbero direttamente dati da un privato. Pertanto, c'è chi ha prospettato come soluzione la possibilità di inserire un obbligo di notifica allo Stato in

pensi all'enorme mole di dati in possesso di *Google* e di *Facebook*. Sul punto, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 720.

⁷⁰⁰ Ad esempio, la posta elettronica di una persona può essere archiviata in un altro Paese da un fornitore di servizi o una persona può archiviare intenzionalmente i dati in un altro Paese. Queste persone possono recuperare i dati e, a condizione che abbiano un potere legittimo, possono divulgare volontariamente i dati alle forze dell'ordine o consentire alle autorità di accedere ai dati, come previsto dall'articolo. Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 294, p. 53.

⁷⁰¹ In tal senso, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 721.

⁷⁰² In tal senso, I. WALDEN, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, in AA.VV., *Privacy and Security for Cloud Computing* (S. PEARSON, G. LEE eds.), Heidelberg, 2012, p. 52; ID., *Law Enforcement Access to Data in Clouds*, in AA.VV., *Cloud Computing Law* (C. MILLARD ed.), Oxford, 2013, p. 295. V., più in generale, C. MILLARD, *Cloud Computing Law*, Oxford, 2021.

⁷⁰³ Cfr., TRANSBORDER GROUP, *Transborder Access and Jurisdiction: What Are the Options?*, Discussion Paper No T-CY(2012)3, Cybercrime Convention Committee, Council of Europe, 6 dicembre 2012, p. 21. Di tale avviso anche, COMMISSIONE EUROPEA, *Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, 2 dicembre 2016, disponibile al link: <https://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf>.

⁷⁰⁴ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #3 – Transborder access to data (Article 32)*, T-CY (2013)7 E, Strasburgo, 3 dicembre 2014, p. 7, disponibile al link: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a>.

cui ha sede il privato fornitore del dato, la quale consentirebbe di svolgere una funzione di controllo⁷⁰⁵.

Le Parti, inoltre, devono fornire assistenza per la raccolta in tempo reale dei dati relativi al traffico trasmessi attraverso un sistema informatico. I dati relativi al traffico devono riguardare comunicazioni avvenute nel territorio della Parte richiedente.

La disciplina prevista dall'art. 33 si basa su uno sterile rinvio alle condizioni ed alle procedure previste dal diritto interno, specificando che l'assistenza deve essere fornita almeno rispetto ai reati per i quali la raccolta in tempo reale dei dati sul traffico sarebbe possibile, in ambito interno, per una situazione analoga⁷⁰⁶. Pertanto, i termini e le condizioni in base ai quali tale cooperazione deve essere fornita sono generalmente quelli stabiliti nei trattati, accordi e leggi applicabili che disciplinano l'assistenza giudiziaria in materia penale⁷⁰⁷.

Si tratta di un meccanismo che assume particolare rilevanza nel momento in cui l'autorità giudiziaria non possa garantire di risalire alla fonte di una comunicazione seguendo la traccia delle registrazioni delle trasmissioni precedenti, poiché i dati informatici sul traffico non sono più disponibili perché potrebbero essere stati cancellati dal fornitore di servizi o perché l'autore dell'intrusione abbia cessato la sua attività o cambiato il suo percorso di accesso⁷⁰⁸.

Risulta, quindi, di fondamentale importanza per le autorità procedenti ottenere in tempo reale i dati sul traffico relative alle comunicazioni che passano attraverso un sistema informatico situato in altri Stati.

Eadem ratio anche per le intercettazioni dei dati relativi al contenuto, disciplinate all'art. 34 della Convenzione sulla criminalità informatica⁷⁰⁹. Sulle Parti grava un obbligo limitato a causa dell'elevato grado di intrusività dell'intercettazione. Gli Stati devono prestarsi reciproca assistenza per le intercettazioni di comunicazioni che migrino su sistemi informatici collocati in Stati esteri, secondo le modalità consentite dai trattati applicabili e dalle leggi interne, a cui si rinvia.

5. L'ingiunzione di produrre

Gli elementi transfrontalieri non sono individuabili unicamente nel Capitolo III della Convenzione sulla criminalità informatica. Nei precedenti paragrafi, si è avuto modo di appurare come la Convenzione di Budapest affronti le ricerche transfrontaliere unilaterali in due casi limitati: dati disponibili al pubblico (art. 32, lett. a) e divulgazione previo consenso (art. 32, lett. b). Tuttavia, la transnazionalità sembra emergere anche nella disciplina relativa all'ingiunzione di produrre, di cui all'art. 18 della Convenzione in esame.

L'ingiunzione di produrre – altrimenti detta ordine di produzione internazionale – è lo strumento mediante il quale un'autorità può ordinare ad un soggetto la trasmissione di

⁷⁰⁵ Così, J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, cit., p. 721.

⁷⁰⁶ Gli Stati, dunque, possono limitare l'ambito di applicazione della misura nazionale equivalente, nel rispetto del limite posto dalla norma.

⁷⁰⁷ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 295, p. 53.

⁷⁰⁸ A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, cit., p. 7.

⁷⁰⁹ Sul punto, M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 320 ss.

dati informatici⁷¹⁰. Si tratta di una misura flessibile nonché meno intrusiva ed onerosa rispetto alle tradizionali, come la perquisizione informatica ed il sequestro, che consente di ottenere informazioni rilevanti per le indagini con modalità più vantaggiose sia per le autorità giudiziarie sia per i custodi dei dati di terze parti, come gli *Internet Service provider*⁷¹¹ e può precedere l'attività di perquisizione informatica e di sequestro⁷¹².

È importante sottolineare che, sebbene sia una misura procedurale nazionale, può essere utilizzata per ottenere dati informatici all'estero⁷¹³.

L'istituto è contenuto nel Capitolo II dedicato ai provvedimenti da adottare a livello nazionale. Ciò farebbe pensare ad uno strumento che esclude dal proprio raggio di azione elementi aventi attitudine probatoria collocati all'estero. Tuttavia, si è aperta una discussione internazionale relativa all'obbligo dei fornitori di servizi di divulgare dati con un elemento transfrontaliero a seguito dell'emissione di un ordine di produzione, che ha assunto una particolare eco all'interno del Comitato della Convenzione sulla criminalità informatica (T-CY), il quale ha parzialmente chiarito la circostanza con la *T-CY Guidance Note #10 – Production orders for subscriber information*⁷¹⁴.

L'ingiunzione di produrre può essere di due tipi: ordine rivolto ad un soggetto ed ordine rivolto ad un fornitore di servizi.

L'art. 18, par. 1, lett. a) impone agli Stati di adottare misure legislative e di altra natura necessarie a consentire alle autorità competenti l'emissione dell'ordine di trasmettere specifici dati informatici posseduti o controllati dal soggetto a cui l'ordine è rivolto e immagazzinati in un sistema informatico o supporto di memorizzazione dei dati informatici. Diversamente, il par. 1, lett. b) dello stesso articolo consente di ordinare ad un prestatore di servizi che offre le proprie prestazioni sul territorio dello Stato di emissione di fornire i dati in proprio possesso o sotto il suo controllo relativi ad abbonati e concernenti tali servizi.

Questi poteri investigativi devono essere esercitati nel rispetto delle condizioni e delle garanzie previste all'art. 15 della Convenzione sulla criminalità informatica, che comprende tra l'altro «un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e gli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di

⁷¹⁰ Sull'art. 18 della Convenzione sulla criminalità informatica, R.M.F. BARON, *A Critique of the International Cybercrime Treaty*, cit., p. 276; D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, cit., p. 168 ss.; P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, in *Computer Law & Security Review*, 34, 2018, p. 327 ss.; M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 313; A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, cit., p. 5 ss.;

⁷¹¹ Va chiarito che spesso gli *Internet Service Provider* sono disposti ad assistere le autorità di contrasto su base volontaria fornendo dati sotto il loro controllo. Tuttavia, è evidente la loro preferenza per forme di assistenza che abbiano una solida base giuridica, in modo da essere sollevati da ogni responsabilità di tipo contrattuale ed extracontrattuale.

⁷¹² M. KEYSER, *The Council of Europe Convention on Cybercrime*, cit., p. 313.

⁷¹³ Cfr., *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines*, 2020, p. 6, disponibile al link: <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7>.

⁷¹⁴ CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #10 – Production orders for subscriber information (Article 18 Budapest Convention)*, versione rivista adottata dal T-CY a seguito della sedicesima plenaria con procedura scritta il 28 febbraio 2017, Strasburgo, 1 marzo 2017, T-CY(2015)16, disponibile al link: <https://rm.coe.int/16806f943e>.

proporzionalità» nonché «una supervisione giudiziaria o di altra natura purché indipendente, dei motivi che giustifichino l'applicazione e la limitazione del campo di applicazione e della durata del potere o procedura», considerando «l'impatto dei poteri e delle procedure di questa sezione sui diritti, le responsabilità e gli interessi legittimi dei terzi».

I presupposti per l'emissione sia di un ordine rivolto a un soggetto sia di un ordine rivolto a un fornitore di servizi sono quattro: un requisito soggettivo; un requisito territoriale; un requisito oggettivo; un requisito di tipo connettivo.

Partendo dal primo tipo di ordine, quanto al requisito soggettivo, l'art. 18, par. 1, lett. a) individua il destinatario dell'ingiunzione di produrre in un non meglio definito "soggetto". Per soggetto dovrebbe intendersi qualsiasi persona sia fisica sia giuridica. La *Guidance Note* tende a dare un'interpretazione estensiva alla terminologia utilizzata, includendo anche i fornitori di servizi⁷¹⁵.

Il requisito territoriale richiede che la persona sia sul territorio dello Stato ordinante. Ciò non limita l'indagine sino ad escludere i dati informatici collocati all'estero. Ed invero, la presenza sul territorio dello Stato ordinante non escluderebbe la possibilità di produrre dati memorizzati su *server* collocati all'estero, ma producibili dall'interno del territorio dello Stato ordinante⁷¹⁶.

Per quanto attiene al requisito oggettivo, l'ingiunzione di produrre rivolto ad un soggetto ha ad oggetto «specifici dati informatici». La stessa Convenzione all'art. 1, par. 1, lett. b) li definisce come «qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere la funzione». Si tratterebbe di dati memorizzati o esistenti, e non includerebbe dati che non sono ancora venuti ad esistere come dati di traffico o dati di contenuto relativi a comunicazioni future⁷¹⁷.

È evidente come l'ingiunzione potrebbe richiedere, tra le altre cose, contenuti di *e-mail* e chat, video, messaggi vocali, indirizzi IP sia dinamici sia statici, dati di geolocalizzazione e numeri di serie di un dispositivo informatico, la cronologia di ricerca e di navigazione sul *web*⁷¹⁸, poiché non è limitata solo alle informazioni sugli abbonati, ma riguarda qualsiasi tipo di dato informatico⁷¹⁹.

⁷¹⁵ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #10 – Production orders for subscriber information (Article 18 Budapest Convention)*, cit., p. 6.

⁷¹⁶ Sul punto, P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, cit., p. 334.

⁷¹⁷ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 170, p. 29.

⁷¹⁸ C'è chi ritiene che l'ampia formulazione finisca per includere anche dati ultrasensibili come quelli contenuti nelle cartelle cliniche digitalizzate. In tal senso, P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, cit., p. 335.

⁷¹⁹ CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #10 – Production orders for subscriber information (Article 18 Budapest Convention)*, cit., p. 6. Tuttavia, si continua precisando che la nota orientativa riguarda solo la produzione di informazioni sugli abbonati. Secondo la dottrina, ciò potrebbe significare due cose: o che l'inclusione dei prestatori di servizi nel campo di applicazione dell'art. 18, par. 1, lett. a) della Convenzione sulla criminalità informatica è valida solo quando i dati da ordinare sono limitati alle informazioni sugli abbonati o, più probabilmente, il Comitato intende interpretare l'art. 18, par. 1, lett. a) della Convenzione sulla criminalità informatica come base giuridica per obbligare i prestatori di servizi a produrre tutti i tipi di dati, non limitandolo solo alle informazioni sugli abbonati, ma a causa dei limiti del suo mandato oltre i quali non può andare è stato costretto a evitare di spingersi fino a dare tale interpretazione. Così, P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention*

Il requisito di tipo connettivo richiede che il destinatario dell'ordine abbia il possesso o il controllo dei dati immagazzinati in un sistema informatico o in un supporto informatico per la conservazione, nel territorio dello Stato di emissione dell'ingiunzione. Per possesso dei dati deve intendersi il potere che si manifesta in un'attività corrispondente all'esercizio del diritto di proprietà, pur non essendo la persona proprietaria degli elementi informatici. Il controllo, invece, rimanderebbe alla situazione in cui i dati al di fuori del possesso fisico della persona, ma quest'ultima ne può comunque controllare la produzione dall'interno del territorio dello Stato ordinante, mediante un impianto di archiviazione da remoto. È escluso che il concetto di possesso o controllo sia riconducibile alla mera capacità tecnica di accedere a dati memorizzati da remoto⁷²⁰.

Diverso, invece, l'ordine rivolto ad un fornitore di servizi. Da un punto di vista sistematico, si potrebbe affermare che la disciplina prevista per tale ordine sia *lex specialis* rispetto alle regole sull'ordine rivolto a un soggetto.

Ed invero, ai sensi dell'art. 18, par. 1, lett. b), le autorità competenti di uno Stato possono emettere anche un ordine nei confronti di un fornitore di servizi. In tal caso, i requisiti sono parzialmente diversi. Innanzitutto, il destinatario può essere solamente un ente pubblico o privato che «fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico» e qualsiasi altro ente che «processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio»⁷²¹. Tuttavia, la relazione esplicativa chiarisce che i *provider* debbano offrire almeno servizi di comunicazione o di trattamento dei dati correlati⁷²².

Al requisito soggettivo, si affianca il requisito oggettivo. Questo tipo di ordine può essere emesso solo per ottenere dati relativi agli abbonati dell'*internet service provider* o concernenti i servizi prestati. Limitatamente all'ingiunzione a produrre, ai sensi dell'art. 18, par. 3, della Convenzione sulla criminalità informatica, per informazioni relative agli abbonati si intendono le informazioni detenute in forma di dato informatico o sotto altra forma da un fornitore di servizi e relativa agli abbonati o ad un proprio servizio, che sia diversa dai dati relativi al traffico o al contenuto.

Attraverso tali dati deve essere possibile stabilire: il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio; l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio; ogni altra forma di informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio⁷²³. Non è chiarito con precisione, però, cosa possa essere un'informazione sugli abbonati. Tuttavia, pare si possa affermare che i

Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law, cit., p. 333.

⁷²⁰ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 173, p. 29.

⁷²¹ Così, l'art. 1, par. 1, lett. c) della Convenzione sulla criminalità informatica.

⁷²² Secondo tale interpretazione, l'*Internet Service Provider* può essere anche un fornitore di contenuti *over-the-top* (OTT), come Whatsapp, Skype o Telegram. In tal senso, P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, cit., p. 331. V., anche, *Explanatory Report to the Convention on Cybercrime*, par. 27, p. 6.

⁷²³ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 180, p. 31.

dati sull'abbonato sono informazioni per identificare l'utente di uno specifico indirizzo IP o, viceversa, gli indirizzi IP utilizzati da una persona specifica⁷²⁴.

L'art. 18, par. 1, lett. b) della Convenzione sulla criminalità informatica richiede che i dati relativi agli abbonati siano concernenti i servizi offerti dal fornitore. Si tratta di un fattore restrittivo che consente di evitare la diffusione di informazioni sensibili sull'abbonato, nel rispetto del principio di proporzionalità, a garanzia dei diritti fondamentali coinvolti.

Ed invero, se un fornitore di servizi come *Whatsapp*, che consente la comunicazione tramite testo e voce, nonché la condivisione di altri contenuti come immagini, file e documenti, raccoglie informazioni relative agli stili di vita della persona, all'orientamento o vita sessuale, alle opinioni politiche, alla propria religione o credo, non potrà diffondere tali informazioni ai sensi dell'art. 18, par. 1, lett. b) perché non strettamente concernenti i suoi servizi.

Mentre per l'ordine emesso nei confronti di un soggetto è necessario che la persona sia presente sul territorio dello Stato ordinante, per l'ordine emesso nei confronti del fornitore di servizi è necessario che quest'ultimo offra le proprie prestazioni sul territorio dello Stato ordinante. La formulazione del requisito territoriale è ambigua. La crescita del *cloud computing* ha sollevato interrogativi dal momento in cui si ritiene che un *internet service provider* offra i propri servizi nel territorio dello Stato e possa quindi ricevere un ordine di produzione relativo alle informazioni sugli abbonati.

Si sono sviluppate due linee interpretative tra loro contrarie⁷²⁵. Una prima linea di pensiero ritiene che sia consentito allo Stato ordinante di emettere un'ingiunzione di produrre nei confronti di tutti i fornitori di servizi del mondo, poiché, partendo da una interpretazione letterale, si potrebbe sostenere che qualsiasi forma di accessibilità ai servizi del prestatore dall'interno dello Stato sia sufficiente. Un secondo orientamento sostiene la necessaria presenza fisica del prestatore di servizi all'interno dello Stato richiedente, con conseguente esclusione di tutti i prestatori di servizi stranieri⁷²⁶.

Un terzo orientamento è stato avanzato dalla Corte di cassazione belga, la quale, per comprendere se sono offerte prestazioni sul territorio dello Stato richiesto, ha ritenuto sufficiente verificare che il fornitore di servizi svolga attività commerciali su di esso, ad esempio attraverso la pubblicità in lingua nazionale o commercio dei dati raccolti relativi agli utenti⁷²⁷.

Secondo un primo chiarimento del Comitato della Convenzione sulla criminalità informatica sarebbe possibile applicare l'art. 18, par. 1, lett. b) della Convenzione anche

⁷²⁴ In tal senso, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, final report of the T-CY Cloud Evidence Group, Strasburgo, 16 settembre 2016, T-CY(2016) 5, p. 12.

⁷²⁵ Sulla differenza tra proposizioni opposte e proposizioni contrarie, F. CORDERO, *Procedura penale*, cit., p. 375, secondo cui «[d]a Ermagora a Quintiliano, la teoria degli “status causae” descrive figure dialettiche a battute opposte o contrarie [...]. Date due proposizioni, le definiamo opposte quando abbiano lo stesso tema e una sia preceduta dal segno “non” (o “è falso che...”); una deve essere vera, anzi lo è, perché p e non-p esauriscono l'universo logico; impossibile che siano tutt'e due false [...] (tertium non datur). Sono contrarie quando, se una fosse vera, l'altra sarebbe falsa, ma niente esclude che siano entrambe false [...]».

⁷²⁶ Così, P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, cit., p. 332.

⁷²⁷ Hof Van Cassatie van België, 1° dicembre 2015, nr. P.13.2082.N, *Yahoo!*, par. 8, in *Digital Evidence and Electronic Signature Law Review*, 13, 2016, p. 156 ss., disponibile al link: <https://journals.sas.ac.uk/deeslr/article/view/2310/2261> (testo tradotto in lingua inglese).

nelle ipotesi in cui l'*Internet service provider* che offre i propri servizi nello Stato ordinante non sia presente né fisicamente né legalmente sul territorio. Tuttavia, è necessaria una doppia valutazione per determinare se è soddisfatto l'obbligo di offrire i propri servizi sul territorio: possibilità di abbonarsi ai servizi da parte delle persone presenti sul territorio dello Stato ordinante; vincolo connettivo reale e sostanziale con lo Stato da valutare sulla base di determinati fattori rilevanti⁷²⁸.

Si è quindi optato per un'interpretazione innovativa che tenga conto del collegamento commerciale aggiuntivo da parte del prestatore di servizi, anche straniero, con lo Stato di emissione dell'ingiunzione. Tuttavia, non va sottaciuto che tale tecnica trascura aspetti fisici della territorialità a vantaggio di un "collegamento virtuale".

Sembra, dunque, potersi affermare con un ampio margine di certezza che le autorità preposte possano inviare un ordine di produzione per i dati dell'abbonato anche a un fornitore di servizi che non ha sede in uno Stato ordinante ma che offre i propri servizi su quel territorio⁷²⁹.

Infine, anche per l'emissione di quest'ordine è previsto il requisito di tipo connettivo del possesso o controllo dei dati da parte del fornitore di servizi, limitatamente alle sole informazioni producibili, relative ai proprio abbonati e concernenti i servizi prestati.

Per quanto riguarda le modalità di produzione, le Parti potrebbero stabilire l'obbligo di produrre i dati informatici o le informazioni sull'abbonato secondo le modalità indicate nell'ordine. Si potrebbe far riferimento a un periodo di tempo entro il quale deve essere effettuata la divulgazione, o alla forma, o alle modalità di produzione (ad esempio si può ordinare che i dati o le informazioni siano forniti in "testo normale", online o su carta stampata o su un supporto informatico quale compact disc, penna usb, ecc.)⁷³⁰.

Lo strumento descritto, ad oggi, soffre di alcuni limiti che non consentono un utilizzo sereno e pacifico. La dottrina straniera ha evidenziato come un rafforzamento degli interessi pubblicistici e della sicurezza non trovi un bilanciamento nella protezione dei diritti fondamentali e nel rispetto degli interessi della sovranità statale⁷³¹. Purtroppo, il quadro giuridico internazionale non è ancora sufficientemente chiaro, preciso ed efficiente, mentre il progresso tecnologico continua ed è ormai inarrestabile.

In Italia, l'ingiunzione di produrre troverebbe la propria base giuridica nell'art. 132, comma 3, d. lgs. 30 giugno 2003, n. 196⁷³². L'articolo non distingue i dati sugli abbonati

⁷²⁸ Per stabilire se sussiste la connessione reale e sostanziale si valutano alcuni fattori rilevanti tra cui la misura in cui l'*Internet service provider* orienta le proprie attività nei confronti degli abbonati (ad esempio, fornendo pubblicità locale o pubblicità nella lingua parlata sul territorio dello Stato), utilizza le informazioni sull'abbonato o i dati sul traffico durante lo svolgimento delle sue attività, interagisce con gli abbonati presenti sul territorio dello Stato o può altrimenti essere considerato stabilito sul territorio dello Stato. Il solo fatto che un fornitore di servizi utilizzi un nome di dominio o un indirizzo di posta elettronica collegato a un determinato Paese non fa presumere che la sua sede di attività sia situata in quello Stato. Inoltre, il requisito può essere soddisfatto anche se l'*Internet service provider* fornisce servizi con un nome di dominio che fa riferimento a un altro Paese. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #10 – Production orders for subscriber information (Article 18 Budapest Convention)*, cit., p. 8.

⁷²⁹ Cfr., *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines*, 2020, p. 6 e 37, disponibile al link: <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7>.

⁷³⁰ Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 176, p. 30.

⁷³¹ In tal senso, P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, cit., p. 335.

⁷³² A sostegno di tale tesi, si veda quanto indicato sulla piattaforma *Octopus* sviluppata nell'ambito del Consiglio d'Europa, alla sezione "Public/private cooperation" disponibile al link:

e i dati sul traffico. Tuttavia, alcuni *provider* ritengono di poter fornire i dati dell'abbonato (piuttosto che i dati sul traffico) anche su richiesta della polizia giudiziaria⁷³³.

Sotto il profilo strettamente procedurale, in passato, l'acquisizione dei dati avveniva a seguito dell'emissione di un decreto motivato della Procura della Repubblica, anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, dell'offeso e delle altre persone private. Anche il difensore dell'imputato o della persona sottoposta alle indagini poteva chiedere direttamente al fornitore i dati, limitatamente alle utenze intestate al proprio assistito, con le modalità previste all'art. 391-*quater* c.p.p., purché la mancata acquisizione avrebbe potuto provocare un pregiudizio concreto ed effettivo allo svolgimento delle investigazioni difensive⁷³⁴.

Di recente, in tema di *data retention* è intervenuta la Corte di giustizia, con la nota sentenza H.K.⁷³⁵, ove i giudici hanno stabilito che l'accesso di autorità pubbliche ad un

https://www.coe.int/en/web/octopus/-/ita-1?redirect=https://www.coe.int/en/web/octopus/information-on-parties?p_p_id=101_INSTANCE_dW5sR9Hp7iGb&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_count=1.

⁷³³ In Francia, invece, la polizia giudiziaria può ordinare a qualsiasi persona o ente pubblico o privato di produrre qualsiasi informazione in suo possesso rilevante ai fini dell'indagine anche in formato digitale (art. 60-1 del codice di procedura penale). Inoltre, la polizia giudiziaria può ordinare in forma elettronica a qualsiasi persona giuridica o ente pubblico di mettere a disposizione qualsiasi informazione che accerti la verità, contenuta nei propri sistemi informatici o nel suo sistema relativo al trattamento dei dati personali (art. 60-2 del codice di procedura penale).

Più articolata la disciplina adottata dallo Stato tedesco. In Germania, per gli ordini di cui all'art. 18, par. 1, lett. a) della Convenzione sulla criminalità informatica l'autorità competente è il magistrato del pubblico ministero o il tribunale per quanto riguarda i dati informatici, mentre i dati sugli abbonati può richiederli anche la polizia. Diversamente, per gli ordini di cui all'art. 18, par. 1, lett. b) della Convenzione sulla criminalità informatica l'autorità competente è il tribunale, mentre nei casi di urgenza che non riguardano i dati detenuti obbligatoriamente, può emettere un ordine anche il magistrato del pubblico ministero. I dati informatici possono essere ottenuti mediante un ordine di produzione, come previsto alla Sezione 95 del codice di procedura penale. Invece, la raccolta delle informazioni sugli abbonati, quali dati del cliente, compreso il nome, l'indirizzo e i codici di identificazione, è consentita se l'ordine è emesso nei confronti delle imprese di telecomunicazioni, a condizione che ciò sia necessario per le indagini sul caso o per l'individuazione del luogo in cui si trova il sospettato (sezione 100j del codice di procedura penale). Tale procedura si applica solo se sussiste un sospetto iniziale di reato. Infine, i dati sul traffico possono essere ottenuti tramite un ordine di produzione in conformità con quanto stabilito dalla sezione 100g del codice di procedura penale. La sezione 100g (1) del codice di procedura penale richiede quali presupposti che si tratti di un reato qualificato come significativamente importante, non solo perché così qualificato in astratto, ma anche con riferimento alle circostanze del singolo caso concreto ovvero che sia stato commesso un reato che utilizza le telecomunicazioni. Se l'ordine si riferisce a dati sul traffico che devono essere conservati dalle imprese di telecomunicazioni per un certo periodo in conformità con la legge che introduce l'obbligo di conservazione dei dati, entrata in vigore il 18 dicembre 2015, la raccolta è consentita solo in caso di reati particolarmente gravi, elencati nella sezione 100g (2) del codice di procedura penale. Di regola, tutti gli ordini devono essere inviati in forma scritta.

Per ulteriori informazioni sulle misure adottate dalle Parti contraenti relative all'ingiunzione di produrre, si rinvia al sito web dell'*Octopus Cybercrime Community*: <https://www.coe.int/en/web/octopus/information-on-parties>.

⁷³⁴ Così, G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 1606; P. TONINI, C. CONTI, *Il diritto delle prove penali*, Milano, 2014, p. 469.

⁷³⁵ Corte di giustizia, Grande Sezione, 2 marzo 2021, causa C-746/18, H.K. La pronuncia non costituisce un *dictum* isolato, bensì, si inserisce, nel vorticoso «tsunami comunitario» provocato dalle precedenti pronunce *Digital Rights* del 2014 e *Tele 2 Sverige* del 2016. Cfr., Corte di giustizia, Grande Sezione, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*; Corte di giustizia, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB*. In dottrina, S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1586 ss.

insieme di dati relativi al traffico o di dati relativi all'ubicazione, idonei a fornire informazioni sulle comunicazioni effettuate da un utente di un mezzo di comunicazione elettronica o sull'ubicazione delle apparecchiature terminali da costui utilizzate e a permettere di trarre precise conclusioni sulla sua vita privata, per finalità di prevenzione, ricerca, accertamento e perseguimento di reati, deve essere circoscritto a procedure aventi per scopo la lotta contro le forme gravi di criminalità o la prevenzione di gravi minacce alla sicurezza pubblica. Inoltre, hanno chiarito che l'ufficio del pubblico ministero non può essere legittimato ad autorizzare l'accesso di un'autorità pubblica ai dati relativi al traffico e ai dati relativi all'ubicazione ai fini di un'istruttoria penale.

Sulla scorta di tale sentenza, per garantire, con necessità ed urgenza, la possibilità di acquisire i dati esterni alle comunicazioni e, al contempo, il rispetto dei principi enunciati dal recente arresto della Corte di giustizia, il legislatore è intervenuto con d.l. 30 settembre 2021, n. 132, convertito, con modificazioni, in l. 23 novembre 2021, n. 178, modificando la disciplina prevista all'art. 132, d.lgs. 30 giugno 2003, n. 196. La nuova procedura prevede che, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private, il giudice emetta un decreto motivato che autorizza l'acquisizione dei dati, sul presupposto che sussistano sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'articolo 4 del codice di procedura penale, e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti⁷³⁶.

⁷³⁶ Per una completa ricostruzione, G. BATTARINO, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021, n. 132*, in *Questione giustizia*, 5 ottobre 2021; R. BERTUOL, *La nuova disciplina per l'acquisizione dei tabulati telefonici: l'interpretazione "autentica" del Legislatore e la parola fine alla (fin troppo) lunga querelle giurisprudenziale*, in *Giurisprudenza Penale Web*, 12, 2021, p. 1 ss., disponibile al link: https://www.giurisprudenzapenale.com/wp-content/uploads/2021/12/Bertuol_gp_2021_12.pdf. Sui recenti sviluppi, ex multis, J. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema Penale*, 29 aprile 2021; L. GIORDANO, *La Corte di Cassazione ritorna sull'acquisizione dei tabulati telefonici dopo le indicazioni della CGUE*, in *ilPenalista.it*, 5 ottobre 2021; M. LANDOLFI, *La Corte di Giustizia UE interviene ancora sulla conservazione e sull'accesso ai dati di traffico e di ubicazione: alcune riflessioni sulla disciplina interna (prima parte)*, in *Studium Juris*, 12, 2021, p. 1481 ss.; A. MALACARNE, *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m.*, in *Sistema penale*, 5 maggio 2021; A. MARANDOLA, *I tabulati, un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, in *Studium Iuris*, 11, 2021, p. 1328 ss.; W. NOCERINO, *La nuova (e incompleta) disciplina dei tabulati telefonici in Italia*, cit., p. 1 ss., disponibile al link: <https://intelligencesecurityinvestigation.it/la-nuova-e-incompleta-disciplina-dei-tabulati-telefonici-in-italia/>; C. PARODI, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in *ilprocessotelematico.it*, 25 maggio 2021; F. RINALDINI, *Data retention e procedimento penale. Gli effetti della sentenza della Corte di giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore*, in *Giurisprudenza penale web*, 11 maggio 2021; G. STAMPANONI BASSI, *Acquisizione dei tabulati telefonici: anche la Corte di Assise di Napoli esclude una applicazione diretta della sentenza CGUE del 2 marzo 2021 (C-746/18)*, in *Giurisprudenza penale web*, 17 giugno 2021; V. TONDI, *La disciplina italiana in materia di data retention a seguito della sentenza della Corte di giustizia UE. Il tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema penale*, 7 maggio 2021.

6. Luci ed ombre della Convenzione sulla criminalità informatica. Verso un Secondo protocollo

Con il tempo, la Convenzione sulla criminalità informatica ha raccolto un'ampia adesione. Oggi ha un impatto in tutte le regioni del mondo, tanto da rappresentare non solo un documento legale – che prevede regole relative alla criminalità informatica, regole procedurali che assicurano le prove elettroniche e una buona base giuridica per la cooperazione internazionale – ma un vero e proprio quadro raffigurante la completa panoramica relativa alla criminalità informatica.

Invero, ogni Stato può utilizzare la Convenzione come linea guida per la legislazione nazionale ovvero diventarne parte. In tale ultimo caso, si schiude un ventaglio di importanti benefici per lo Stato aderente, il quale potrà utilizzare la Convenzione come base legale per la cooperazione internazionale; avere un ruolo attivo nella formazione di note orientative e protocolli addizionali necessari per l'ulteriore evoluzione della Convenzione; essere parte della rete di professionisti – la Rete 24/7 – designando un punto di contatto; sperimentare nuove attività di cooperazione diretta con il settore privato.

È considerato, quindi, l'accordo internazionale più rilevante in materia, poiché rappresenta attualmente lo strumento di riferimento che consente ai professionisti di tutto il mondo di condividere esperienze e creare relazioni che facilitano la cooperazione in casi specifici ed in situazioni di emergenza, anche grazie al sostegno della Commissione per la Convenzione sulla criminalità informatica (T-CY) e del *Cybercrime Programme Office* (C-PROC)⁷³⁷.

Come qualsiasi prodotto creato dall'uomo, la Convenzione non apporta solo benefici, ma tradisce molteplici criticità, frutto dell'imperfezione umana. Tuttavia, non bisogna muovere alcun rimprovero, poiché è dall'imperfezione che nasce l'evoluzione, e da questa, il miglioramento sociale e giuridico. Il riferimento va ovviamente al recente secondo protocollo di cui si discuterà soltanto dopo aver evidenziato i punti di forza e di debolezza di una Convenzione tanto essenziale quanto centrale per la lotta a tutte le forme di criminalità che in qualche modo utilizzano elementi e strumenti informatici.

Seppur portatrice di evidenti vantaggi, gli Stati hanno sottolineato come gli strumenti di mutua assistenza previsti dalla Convenzione abbiano un'efficacia limitata. Pertanto, si è ritenuto necessario migliorare le procedure previste in caso di indagini relative alla criminalità informatica transnazionale e per la formazione delle prove elettroniche.

Sebbene la Convenzione non abbia risolto tutti i problemi, ha comunque aiutato a migliorare le attività di cooperazione, contribuendone al successo. Invero, alcuni Stati – generalmente piccoli e poveri – hanno evidenziato come l'adesione alla Convenzione abbia migliorato i rapporti con le autorità straniere perché vincolati a fornire assistenza, laddove in passato, in assenza di Accordi bilaterali, non si riusciva ad ottenere una proficua forma di collaborazione.

Sebbene la Convenzione rimanga un importante punto di riferimento nell'individuazione delle regole relative alla cooperazione internazionale per la formazione delle prove elettroniche, la Commissione per la Convenzione sulla criminalità

⁷³⁷ In tal senso, CYBERCRIME CONVENTION COMMITTEE (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, T-CY (2020)16, cit., p. 3. La Commissione per la Convenzione sulla criminalità informatica (T-CY) ritiene che i vantaggi relativi alla cooperazione giudiziaria derivino dal completo quadro giuridico rappresentato dalla Convenzione. Infatti, il capitolo sulla cooperazione internazionale contiene disposizioni generali individuabili anche in altri trattati di cooperazione in materia penale, nonché specifiche disposizioni per la raccolta di prove elettroniche.

informatica (T-CY), in applicazione dell'art. 46 della Convenzione sulla criminalità informatica, ha ritenuto necessario istituire nel tempo nuovi gruppi di lavoro come il *Transborder Group* ed il *Cloud Evidence Group*⁷³⁸ allo scopo di studiare la cooperazione internazionale e l'accesso alle prove elettroniche nel ciberspazio, adottando diversi rapporti⁷³⁹.

È apparso evidente che, da sola, la Convenzione non era in grado di garantire efficienza. Seppur fornisca una base sufficiente, è stato necessario implementare ulteriori atti che fungessero da strumenti di orientamento, soprattutto nei rapporti tra pubblico e privato. Mentre la Convenzione e le legislazioni nazionali rappresentano la base per la cooperazione, tutti i dettagli tecnici, i canali di cooperazione, le attività congiunte di sensibilizzazione e formazione, devono essere regolati⁷⁴⁰ con le linee guida⁷⁴¹, con gli

⁷³⁸ Tra le principali sfide individuate dal *Cloud Evidence Group* vi erano quelle relative al *cloud computing*, alla territorialità e alla giurisdizione, strettamente legate alle difficoltà di ottenere un accesso efficiente alle prove elettroniche o alla loro divulgazione. Queste problematiche sono, infatti, state affrontate prima nel *Transborder Group* tra il 2012 ed il 2014, mentre dal *Cloud Evidence Group* dal 2015 al 2017. Sull'argomento, si veda anche, COUNCIL OF EUROPE, *Enhanced international cooperation on cybercrime and electronic evidence: towards a protocol to the Budapest Convention*, 14 aprile 2021, disponibile al link: <https://rm.coe.int/towards-2nd-additional-protocol/1680a22487>.

⁷³⁹ Uno dei primi rapporti è stato il *Transborder Access to Data and Jurisdiction: what are the options?*, adottato nel dicembre 2012 e disponibile al link <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8>. Nel rapporto del *Transborder Group* del 2013 sono state poste le basi per il secondo protocollo aggiuntivo alla Convenzione di Budapest. Il rapporto è rinvenibile al link <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e712e>. Successivamente, sono state discusse nuove opzioni per rispondere alle esigenze emerse nel corso delle riunioni del *Cloud Evidence Group*. A tal proposito, nel dicembre 2014 è stato pubblicato il *Transborder access to data and jurisdiction: Options for further action by the T-CY* e recuperabile al link <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e>. Inoltre, si sono tenuti diversi dibattiti sulle prove elettroniche conservate nei *cloud* e sulle relative sfide, con l'obiettivo di trovare soluzioni sia legislative che pratiche. Per un resoconto, si vedano il *Criminal Justice access to data in the cloud: challenges*, del maggio 2015, disponibile al link <https://rm.coe.int/1680304b59>; il *Criminal justice access to electronic evidence in the cloud – Informal summary of issues and options under consideration by the Cloud Evidence Group*, del febbraio 2016, disponibile al link <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8>; il *Criminal justice access to data in the cloud: cooperation with "foreign" service providers* del maggio 2016, disponibile al link <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064b77d>. Intanto, nel settembre 2016, il T-CY ha preparato il rapporto *Criminal justice access to data in cloud: Recommendations for consideration by the T-CY* che includeva raccomandazioni per ulteriori azioni e pubblicato al link <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>. Nel 2017 sono cominciate le discussioni sull'applicazione dell'art. 18 della Convenzione, che hanno portato all'adozione della *T-CY Guidance Note #10 Production Orders for subscriber information (Article 18 Budapest Convention)*, rinvenibile al link <https://rm.coe.int/16806f943e>.

⁷⁴⁰ Per uno studio di carattere generale sul tema, si consulti lo studio cofinanziato dall'Unione europea e dal Consiglio d'Europa, *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines*, rinvenibile al link: <https://rm.coe.int/2088-33-law-enforcement-isp-guidelines-2020/1680a091a7>.

⁷⁴¹ Tra le linee guida più importanti, si possono ricordare quelle elaborate da Facebook, da Apple e da Google. Ad esempio, Whatsapp ha elaborato linee guida destinate ai rappresentanti delle forze dell'ordine che richiedono informazioni. In aggiunta alle linee guida, i rappresentanti delle forze dell'ordine possono anche inviare eventuali domande o contattare Whatsapp in situazioni di emergenza. In particolare, per i procedimenti legali negli Stati Uniti d'America, la società rilascia i dati solo nel rispetto delle condizioni d'uso dell'applicazione e delle leggi applicabili, compreso lo *Stored Communications Act* ("SCA"), sezioni

accordi di cooperazione con gli *Internet service providers* e con i *Memorandum di cooperazione* (MoU)⁷⁴².

In particolare, le linee guida per la cooperazione tra fornitori di servizi e forze dell'ordine adottate alla Conferenza *Octopus* sulla cooperazione contro la criminalità informatica tenutasi il 1° e il 2 aprile 2008 a Strasburgo⁷⁴³: prevedono linee guida comuni sia per le forze dell'ordine che per i fornitori di servizi e linee guida specifiche per ciascuno di essi; non sostituiscono la legislazione penale o altri regolamenti formali, ma li integrano e li aiutano a funzionare nella pratica; si basano sulle buone pratiche; devono essere adattate alle circostanze specifiche di ogni Stato. In pratica, esse assumono la funzione di modelli o "fonti di ispirazione" per le autorità nazionali al fine di migliorare e facilitare la cooperazione con il settore privato⁷⁴⁴.

A ogni buon conto, molte informazioni possono essere considerate superate. Infatti, col trascorrere degli anni e con i rilevanti progressi tecnologici, le linee guida sono diventate obsolete. Invero, col tempo si sono sviluppati il *cloud storage*, le criptovalute, i mercati neri su internet che hanno consentito un aumento della percentuale di crimini commessi su internet, e, al tempo stesso, hanno messo a dura prova le forze dell'ordine, colte impreparate innanzi a tali sistemi informatici avanzati, con conseguente sfiducia nelle forze dell'ordine, poco preparate nelle attività di identificazione dei criminali e di apprensione degli elementi di prova informatici dai fornitori di servizi⁷⁴⁵.

2701-2712 dell'U.S.C. (*United States Code*, codice degli Stati Uniti) titolo 18. Per quanto attiene ai procedimenti legali internazionali, la società si riserva di valutare se le richieste sono coerenti con gli *standard* riconosciuti a livello internazionale, inclusi i diritti umani, il giusto processo e lo stato di diritto. Potrebbe essere necessaria una richiesta di *Mutual Legal Assistance Treaty* (trattato di mutua assistenza giudiziaria) o una rogatoria per ottenere il rilascio dei contenuti di un *account*. Qualora siano necessari il rilascio immediato di informazioni e l'intervento in caso di pericolo imminente per un bambino o rischio di morte o serio danno fisico a una persona, un rappresentante delle forze dell'ordine può inviare una richiesta tramite il Sistema per le richieste online delle forze dell'ordine di Whatsapp, specificando che si tratta di una ipotesi di emergenza. Le linee guida di Whatsapp sono disponibili al link: <https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities/?lang=it>.

⁷⁴² I *Memorandum* di cooperazione prevedono l'istituzione di gruppi di lavoro tra rappresentanti delle forze dell'ordine e dei fornitori di servizi con l'obiettivo di raggiungere un'intesa o anche un accordo formale di cooperazione. Tuttavia, la crescita esponenziale del *cloud storage*, affiancata all'aumento della criminalità internazionale, ha prodotto un significativo aumento delle richieste ai fornitori di servizi multinazionali. I fornitori di servizi internazionali hanno espresso alcune preoccupazioni perché notano, tra le altre cose, l'assenza di familiarità con i sistemi informatici ed i servizi da loro erogati da parte delle forze dell'ordine nonché una scarsa qualità delle richieste, perché spesso incomplete.

⁷⁴³ La Conferenza del 2008 si è concentrata sulla cooperazione tra fornitori di servizi e forze dell'ordine, sullo stato della legislazione sulla criminalità informatica e sull'efficacia della cooperazione internazionale. All'ordine del giorno vi era la valutazione relativa allo stato e all'efficacia della legislazione sulla criminalità informatica, un approfondimento relativo all'identificazione di nuove minacce di criminalità informatica e lo studio del funzionamento dei punti di contatto 24 ore su 24, 7 giorni su 7. La conferenza è stata aperta a coloro che sono professionalmente coinvolti in questioni relative alla criminalità informatica, tra cui: i funzionari della giustizia penale e delle forze dell'ordine, inclusi punti di contatto 24 ore su 24, 7 giorni; i rappresentanti di ministeri, parlamenti o altre istituzioni coinvolte nella legislazione sulla criminalità informatica; i rappresentanti del settore privato, compresi in particolare i fornitori di servizi, le organizzazioni internazionali; le organizzazioni non governative e ricercatori. Per un breve resoconto della conferenza, v., <https://www.coe.int/en/web/cybercrime/ocotpus-interface-2008>.

⁷⁴⁴ Le linee guida sono state utilizzate in molti Paesi, sono state usate per promuovere la cooperazione pubblico-privato in progetti di sviluppo delle capacità e sono state anche approvate dalla Corte europea dei diritti umani.

⁷⁴⁵ Probabilmente le sfide più importanti per le autorità in futuro saranno lo sviluppo e l'uso dell'intelligenza artificiale, gli ulteriori progressi nell'uso della crittografia in un insieme più ampio di

Si è tuttavia assistito ad un aumento esponenziale delle richieste di dati da parte delle forze dell'ordine, con alcuni Paesi – quali gli Stati Uniti d'America – che sono stati letteralmente inondati di richieste di conservazione e produzione di dati, nonché di rimozione di materiale illegale.

Pertanto, sia il quadro legislativo che i meccanismi di cooperazione devono tenere il passo con i nuovi sviluppi. Poiché, oltre a nuove opportunità, queste tecnologie porteranno anche nuove minacce e potrebbero essere usate per scopi malevoli. Le autorità preposte all'applicazione della legge devono essere preparate ad affrontare le nuove minacce ed essere pronte a cooperare con i fornitori di servizi pertinenti.

Il vero nodo da affrontare è relativo alla sede dei fornitori di servizi multinazionali. Nel tempo, si è compreso che le vere difficoltà investigative risiedono nell'assenza di regole chiare e precise relative alla giurisdizione, all'individuazione della legislazione da rispettare nonché ai ruoli ed alle responsabilità dei singoli Stati. È pacifico che i fornitori di servizi debbano rispettare le leggi sulla privacy e la protezione dei dati personali, nonché che debbano rispettare gli obblighi relativi alla cooperazione con le forze dell'ordine. Eppure, ciò che non risulta essere sempre chiaro è l'individuazione della specifica regola da applicare al caso concreto nonché le modalità con cui queste vanno applicate, soprattutto quando si discute di cooperazione e formazione delle prove elettroniche nonché nei casi in cui il reato abbia una natura transfrontaliera.

Ed è qui che si manifestano tutte le imperfezioni della Convenzione sulla criminalità informatica. È stato evidenziato come il sistema di mutua assistenza in vigore da decenni previsto dalla Convenzione sulla criminalità informatica non si è rivelato uno strumento efficace per affrontare le sfide poste dalla raccolta dei dati informatici e dalle prove elettroniche, a causa della facilità con cui i dati salvati sui dispositivi possono essere manipolati, cambiati, spostati o cancellati in breve tempo. Il quadro normativo richiede la comunicazione tra autorità centrali o diplomatiche e comporta molta burocrazia. Pertanto, non può essere usato efficacemente per indagare sulla criminalità cibernetica o su altri reati connessi al ciber spazio⁷⁴⁶.

tecnologie rispetto al presente e le nuove sfide poste dall'uso delle criptovalute, in particolare l'identificazione dei criminali all'una o all'altra estremità delle transazioni. Tali tecnologie, da un lato, aprirebbero a nuove opportunità per fornire ulteriori servizi, per automatizzare diversi processi, creare nuovi prodotti e aumentare la sicurezza e la privacy, dall'altro, potrebbero anche portare ulteriori sfide e ostacoli per le forze dell'ordine. Si pensi all'uso dell'intelligenza artificiale: questa potrebbe portare ulteriori opportunità per combattere il crimine nonché per prevenire e affrontare gli attacchi informatici, ma potrebbe anche creare nuovi strumenti e *modus operandi* per i criminali informatici. Anche la crittografia potrebbe essere usata dal crimine informatico per scopi malevoli. Infatti, se da una parte è utilizzata per garantire la sicurezza delle informazioni e la sicurezza informatica, e può essere usata per proteggere i dati personali e la segretezza delle comunicazioni, dall'altra, può essere un valido strumento utile a preparare o commettere un crimine, creando notevoli difficoltà alle forze dell'ordine legate all'accesso ai dati. Le criptovalute e, più in generale, le valute virtuali sono diventate un mezzo di pagamento e sono utilizzate per scopi di investimento e commercio. Come qualsiasi tipo di valuta, anche queste possono essere un bersaglio per i criminali che possono cercare di rubare o compiere altri reati mediante l'uso di tale moneta.

⁷⁴⁶ Così, CYBERCRIME CONVENTION COMMITTEE (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, T-CY (2020)16, cit., p. 6, la quale sottolinea come nel momento in cui il Paese richiedente prepara la richiesta e la trasmette al Paese ricevente, i dati informatici necessari potrebbero già essere persi. Anche se le autorità possono rapidamente adottare misure volte alla conservazione dei dati informatici, l'effettiva produzione o divulgazione dei dati potrebbe richiedere molto tempo. Quando i dati informatici sono stati finalmente ottenuti, potrebbero essere diventati inutili o obsoleti a causa del tempo trascorso.

Per ovviare alle criticità esposte, molti Stati hanno adottato il sistema della cooperazione diretta, consistente nel diretto invio di ordini di conservazione e produzione ai fornitori di servizi stabiliti all'estero.

Innanzitutto a tale fenomeno, siccome la criminalità è ormai considerata da molte parti una seria minaccia ai diritti umani, allo stato di diritto e al funzionamento delle società democratiche, si è deciso di provvedere alla redazione di un secondo protocollo aggiuntivo alla Convenzione di Budapest sulla criminalità informatica⁷⁴⁷.

La redazione del secondo protocollo è avvenuta in larga parte durante la pandemia da Covid-19. Tale evento ha ulteriormente esacerbato i problemi già noti. Invero, durante l'emergenza sanitaria ricorrere al digitale è diventato indispensabile⁷⁴⁸. Accanto a importanti occasioni di crescita per l'intera società, si è floridamente sviluppata la criminalità informatica, forte di una grande capacità di adattamento. Poiché gli individui, le imprese e i governi sono diventati maggiormente dipendenti dall'uso della tecnologia dell'informazione nelle restrizioni legate alla pandemia, il crimine informatico è risultato in aumento, rendendo maggiormente evidente la necessità di una cooperazione più efficiente⁷⁴⁹.

7. I lavori preparatori del Secondo protocollo

Nel solco del contesto poc'anzi illustrato, il Consiglio d'Europa ha lavorato all'adozione di un secondo protocollo addizionale alla Convenzione sulla criminalità

⁷⁴⁷ Nel Preambolo al Secondo protocollo alla Convenzione sulla criminalità informatica si riconosce espressamente il crescente uso delle tecnologie dell'informazione e della comunicazione e la crescente criminalità informatica, che rappresenta una minaccia per la democrazia e lo Stato di diritto ed è considerata da molti Stati una minaccia ai diritti umani.

⁷⁴⁸ Secondo uno studio, la digitalizzazione dei modelli di lavoro è stata accelerata dalla pandemia da Covid-19, durante la quale si è registrato un aumento del traffico di internet del 60%, mentre sarebbe passato al telelavoro il 40% dei lavoratori dell'Unione europea. Ciò si è evidentemente tradotto in un aumento della vulnerabilità agli attacchi informatici. Secondo la Commissione europea, circa i due quinti degli utenti stanziati nell'Unione europea avrebbero sperimentato problemi di sicurezza ai sistemi informatici, mentre negli ultimi tre anni un terzo degli utenti avrebbe ricevuto e-mail o telefonate fraudolente in cui si richiedevano dati personali. Cfr., Comunicazione congiunta al Parlamento europeo e al Consiglio, *“La strategia dell'UE in materia di cibersicurezza per il decennio digitale”*, JOIN(2020)18 final.

⁷⁴⁹ Intervenendo al dibattito “Cybercrime: attacco all'economia” al Salone della Giustizia 2020, Nunzia Ciardi, direttrice del Servizio centrale della Polizia postale e delle Comunicazioni, ha dichiarato: «La pandemia ha aumentato la superficie d'attacco, visto che quello che non potevamo fare fisicamente lo facevamo online, dal lavoro agli acquisti alla sanità». Di conseguenza, i reati informatici sono aumentati esponenzialmente, tanto da aver indotto la Polizia di Stato a «individuare un protocollo specifico, detto Covid rosso, affinché i nostri gangli sul territorio fossero in contatto con i soggetti interessati, allertandoli ad aumentare i loro livelli di sicurezza». Sul punto, si è espressa anche l'Assemblea Parlamentare del Consiglio d'Europa, la quale, con l'*Opinion 299 (2021)* ha osservato che: «*The Assembly notes that since 2001, the exploitation of information technology for criminal purposes has strongly increased. Cybercrime is considered by many States as a serious threat to human rights, the rule of law, and to the functioning of democratic societies and even to national security. Examples of cybercrimes include online sexual violence against children, the theft and misuse of personal data, election interference and other attacks against democratic institutions, attacks against critical State and public service infrastructures, misuse of informational technology for terrorist purposes and during the ongoing Covid-19 pandemic, cyberattacks on hospitals and laboratories developing vaccines, misuse of domain names to promote fake vaccines and treatments, etc.*».

informatica che migliori l'accesso transfrontaliero alle prove elettroniche, agendo anche sulle regole relative al luogo di conservazione dei dati⁷⁵⁰.

Il 26 giugno 2015 l'Assemblea parlamentare del Consiglio d'Europa ha adottato la Raccomandazione 2077(2015)⁷⁵¹ e la Risoluzione 2070(2015)⁷⁵² sul rafforzamento della cooperazione contro il terrorismo informatico e altri attacchi su larga scala in internet. Con la Raccomandazione 2077(2015), le Parti della Convenzione sulla criminalità informatica sono state invitate a redigere un protocollo aggiuntivo sull'assistenza reciproca in materia di poteri investigativi e a studiare all'interno del *Cloud Evidence Group* la fattibilità della redazione di un secondo protocollo aggiuntivo alla Convenzione sulla criminalità informatica relativo all'accesso della giustizia penale ai dati contenuti nei *cloud servers*. Con la Risoluzione 2070(2015), l'assemblea ha espresso la necessità di un quadro normativo utile ad affrontare adeguatamente le nuove sfide e rendere sicure le prove elettroniche.

I lavori sono ufficialmente iniziati il 7 giugno 2017, quando la Commissione per la Convenzione sulla criminalità informatica (T-CY), nel corso della sua 17ª sessione, ha adottato il mandato per la preparazione del secondo protocollo addizionale, a seguito delle proposte del *Cloud Evidence Group*⁷⁵³.

Il T-CY ha istituito una plenaria per la redazione del protocollo (PDP)⁷⁵⁴, composta dai rappresentanti delle Parti della Convenzione, dagli Stati, dalle organizzazioni e dagli organi del Consiglio d'Europa, in qualità di osservatori. Nella preparazione del progetto di protocollo, il PDP è stato assistito dal gruppo di redazione del protocollo (PDG), composto dagli esperti delle parti della convenzione, suddiviso in diversi sottogruppi e gruppi *ad hoc*, ognuno dei quali ha lavorato su disposizioni ed argomenti specifici⁷⁵⁵.

⁷⁵⁰ Sul punto, A. CAMON, *The project devices and digital evidence in Europe*, in M. CAIANIELLO, A. CAMON, *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Milano, 2021, p. 4; T. MAGNO, *Il progetto Evidence e le principali criticità nell'accesso alle prove elettroniche transnazionali in materia penale: quale futuro?*, in *Informatica e diritto*, 2, 2016, p. 152; R. PEZZUTO, *Accesso transfrontaliero alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *Dir. pen. cont.*, 1, 2019, p. 60; V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, in *Dir. pen. cont.*, 2, 2019, p. 452.

⁷⁵¹ La Raccomandazione è consultabile al seguente link: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21976&lang=en>.

⁷⁵² La Risoluzione 2070 (2015) è rinvenibile al link: <https://pace.coe.int/pdf/05ace237cd4e450adc98a24032bccf7d014aa603fa63f572d0108abe343a2a2d/resolution%202070.pdf>.

⁷⁵³ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, final report of the T-CY Cloud Evidence Group, Strasburgo, 16 settembre 2016, T-CY(2016) 5; CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE (C-PROC), *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines*, Bucharest, 2020, p. 8.

⁷⁵⁴ Generalmente, le sessioni plenarie del *Cybercrime Convention Committee* sono organizzate due volte all'anno e si tengono a porte chiuse. L'ordine del giorno, i documenti di lavoro e le relazioni adottate da queste plenarie sono resi pubblici. Tra il settembre 2017 e il maggio 2021, il T-CY ha tenuto dieci plenarie di redazione, 16 riunioni del *Drafting Group* e numerose riunioni dei sottogruppi e gruppi *ad hoc*. Da quanto si evince dai dati pubblicati dal T-CY, a causa delle restrizioni legate alla pandemia da Covid-19, tra marzo 2020 e maggio 2021, si sono tenute più di 65 riunioni in modalità virtuale. Per maggiori approfondimenti, si rinvia alla pagina web <https://www.coe.int/en/web/cybercrime/t-cy-plenaries>.

⁷⁵⁵ Tali modalità di lavoro hanno consentito ai rappresentanti ed agli esperti di contribuire al massimo alla redazione del protocollo e di sviluppare soluzioni innovative. Sul punto, cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on*

I gruppi di lavoro hanno essenzialmente lavorato su quattro principali blocchi relativi a: disposizioni per una mutua assistenza giudiziaria più efficiente⁷⁵⁶; disposizioni che consentano la cooperazione diretta con i fornitori di servizi in altre giurisdizioni per quanto riguarda le richieste di informazioni sugli abbonati, le richieste di conservazione e le richieste di emergenza; un quadro più chiaro e maggiori garanzie in relazione alle prassi esistenti di accesso transfrontaliero ai dati; tutele, compresi i requisiti in materia di protezione dei dati⁷⁵⁷.

Ai lavori ha partecipato anche la Commissione dell'Unione europea, a nome degli Stati parte della Convenzione e contestualmente membri dell'Unione europea, nell'ambito del mandato di negoziazione conferito dal Consiglio dell'Unione europea il 6 giugno 2019.

La presenza della Commissione dell'Unione europea ha avuto un notevole impatto sui risultati. Infatti, tutte le Parti erano consapevoli della necessità di produrre un secondo protocollo addizionale coerente con le proposte normative in fase di negoziato nell'Unione europea in materia di prove digitali. In effetti, tutti gli Stati membri dell'UE fanno parte anche del Consiglio d'Europa e, di conseguenza, non potrebbero assumere obblighi normativi internazionali tra loro disomogenei o confliggenti⁷⁵⁸. Da qui, nasce l'esigenza di un approccio coerente e coordinato non solo all'interno dello spazio di libertà, sicurezza e giustizia, ma anche a livello internazionale⁷⁵⁹.

Nello specifico, la Commissione dell'Unione europea ha posto particolare attenzione al rispetto dei diritti fondamentali e dei principi generali del diritto dell'Unione europea quali sanciti nei Trattati e nella Carta dei diritti fondamentali dell'Unione europea,

enhanced co-operation and disclosure of electronic evidence, Draft Protocol version 3, T-CY (2020)7, 28 maggio 2021, p. 31.

⁷⁵⁶ In particolare, è stato necessario valutare un sistema semplificato per le richieste di mutua assistenza giudiziaria per quanto riguarda le informazioni relative agli abbonati, un nuovo assetto degli ordini di produzione internazionale, la cooperazione diretta tra le autorità giudiziarie per quanto riguarda le richieste di mutua assistenza giudiziaria, le indagini congiunte e le squadre investigative comuni, le richieste in lingua inglese, le audizioni audio/video di testimoni, persone offese ed esperti, le procedure d'emergenza di mutua assistenza giudiziaria.

⁷⁵⁷ Sul punto, v., COMMISSIONE EUROPEA, *relazione alla Raccomandazione di decisione del Consiglio che autorizza la partecipazione ai negoziati su un secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (STCE n. 185)*, COM(2019) 71 final, Bruxelles, 5 febbraio 2019, p. 2.

⁷⁵⁸ In tal senso, R. PEZZUTO, *Accesso transfrontaliero alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 60. Alla medesima conclusione è pervenuta anche la T-CY, durante la Terza Sessione plenaria tenutasi il 28-29 novembre 2018 a Strasburgo. D'altro canto, la stessa Commissione UE ha avuto modo di sottolineare come le proposte riguardanti le prove elettroniche forniscano la base per un approccio coordinato e coerente sia all'interno dell'Unione europea sia da parte dell'Unione europea a livello internazionale, con la debita attenzione alle norme dell'Unione relative al divieto di discriminazione tra gli Stati membri dell'UE e i loro cittadini. Ha inoltre osservato che la conclusione del secondo protocollo addizionale può incidere su norme comuni o modificarne la portata. Cfr., COMMISSIONE EUROPEA, *relazione alla Raccomandazione di decisione del Consiglio che autorizza la partecipazione ai negoziati su un secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (STCE n. 185)*, COM(2019) 71 final, Bruxelles, 5 febbraio 2019, p. 5.

⁷⁵⁹ Si è correttamente affermato che gli obiettivi perseguiti con il secondo protocollo sono «del tutto analoghi a quelli che ispirano le proposte recentemente sviluppate dalla Commissione europea: vengono in particolare in considerazione le esigenze di incremento della rapidità e dell'efficienza della cooperazione in materia di accesso alla prova digitale, da perseguire anche mediante l'instaurazione di forme dirette di contatto tra le autorità competenti dei Paesi che abbiano sottoscritto la Convenzione e il *service provider* stabilito in altro Stato parte». Cfr., V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 452.

compresi la proporzionalità, i diritti procedurali, la presunzione di innocenza ed i diritti della difesa delle persone sottoposte a procedimento penale, nonché il rispetto della vita privata e la protezione dei dati personali e dei dati delle comunicazioni elettroniche in caso di loro trattamento, inclusi i trasferimenti ad autorità di contrasto in Paesi al di fuori dell'Unione europea, e l'osservanza degli obblighi spettanti a tale riguardo alle autorità di contrasto o giudiziarie.

Il lavoro svolto dal T-CY è stato particolarmente intenso⁷⁶⁰. Lo dimostrano anche i sei cicli di consultazioni che ha tenuto con le parti interessate della società civile, dell'industria e con gli esperti di protezione dei dati⁷⁶¹ nonché la consultazione avviata con l'*European Committee on Crime Problems* (CDPC) e il *Consultive Committee of the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data* (T-PD) del Consiglio d'Europa.

Il progetto del secondo protocollo addizionale è stato approvato nel corso della 24^a plenaria del T-CY del 28 maggio 2021⁷⁶². Successivamente, è stato sottoposto al Comitato dei Ministri in vista della sua adozione formale, avvenuta il 17 novembre 2021⁷⁶³, in concomitanza con il ventesimo anniversario della Convenzione sulla criminalità informatica.

⁷⁶⁰ Il processo di negoziazione è stato tutt'altro che facile, perché le questioni relative alla tecnologia dell'informazione oggi si intersecano con tutti gli aspetti della vita e con gli interessi dei singoli Stati, del settore privato e degli individui. Le attività sono state imponenti: alla preparazione dei testi hanno partecipato gli esperti di 66 Stati parti della Convenzione di Budapest, proveniente dall'Africa, dalle Americhe, dall'Asia e dall'Europa. Per risolvere le complesse questioni legate alla territorialità ed alla giurisdizione, e per conciliare l'efficacia delle indagini con le forti tutele richieste sono state necessarie oltre 95 sessioni redazionali, molte delle quali tenutesi con modalità virtuali a causa della pandemia da Covid-19, e sei cicli di consultazioni con le organizzazioni della società civile, gli esperti di protezione dei dati e con rappresentanti del mondo industriale.

⁷⁶¹ Le consultazioni sono avvenute in concomitanza con la conferenza *Octopus* sulla criminalità informatica tenutasi a Strasburgo nel luglio 2018, con gli esperti di protezione dei dati a Strasburgo nel novembre 2018; tramite invito per commenti scritti sulle bozze di articoli nel febbraio 2019; in concomitanza con la conferenza *Octopus* sulla criminalità informatica a Strasburgo nel novembre 2019; tramite invito per commenti scritti su ulteriori bozze di articoli nel dicembre 2020, e nel maggio 2021 tramite osservazioni scritte e una riunione virtuale tenuta il 6 maggio 2021. Alle consultazioni ha preso parte anche la FRA, l'Agenzia dell'Unione europea per i diritti fondamentali. La FRA ha accolto con favore il progetto del Secondo protocollo aggiuntivo, evidenziando come il progetto rispondesse alla necessità di stabilire un quadro giuridico chiaro, prevedibile ed operativo, a sostegno sia della cooperazione internazionale di contrasto alla criminalità informatica sia della raccolta delle prove elettroniche. Inoltre, la FRA ha osservato che il progetto del Secondo protocollo aggiuntivo ha stabilito dei chiari confini giuridici, prestando attenzione ai diritti fondamentali, e in particolare al diritto alla protezione dei dati personali. Il commento scritto dell'Agenzia dell'Unione europea è rinvenibile al link: <https://rm.coe.int/0900001680a2588f>.

⁷⁶² Nel suo discorso di apertura alla ventiquattresima sessione plenaria, il vicesegretario generale del Consiglio d'Europa, Björn Berge, ha affermato: «La Convenzione di Budapest rimane il *gold standard* per la giustizia penale internazionale, quando si tratta di criminalità informatica». Ha, inoltre, sottolineato che «I criminali hanno intensificato le loro attività, sfruttando i cambiamenti nel modo in cui le persone vivono e lavorano, in un momento di disagio e reale vulnerabilità. I dispositivi, le vittime e le prove di questi crimini sono spesso diffusi in più giurisdizioni». Pertanto, il secondo protocollo addizionale «faciliterà indagini più efficaci e garantirà che lo Stato di diritto raggiunga più in profondità il ciber spazio». È possibile leggere la dichiarazione al link: <https://www.coe.int/en/web/deputy-secretary-general/-/deputy-secretary-general-at-the-opening-of-the-plenary-meeting-of-the-cybercrime-convention>.

⁷⁶³ Nel corso della riunione n. 1417-bis del 17 novembre 2021, dopo aver preso atto del parere n. 299 (2021) dell'Assemblea parlamentare, il Comitato dei ministri ha adottato il Secondo Protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione di prove elettroniche. Nel corso della riunione, si è convenuto di ritornare sulla questione dell'ora e del luogo

Le sfide poste all'attenzione del T-CY erano particolarmente complesse. Tra tutte spiccavano quelle relative alla territorialità e alla giurisdizione relative alle prove elettroniche. Problematica è la questione relativa a specifici dati necessari in un'indagine penale che possono essere conservati in giurisdizioni multiple, mutevoli o sconosciute, come le prove *"in the cloud"*. Appariva indispensabile individuare soluzioni per ottenere la divulgazione di tali dati in modo efficace ed efficiente ai fini di specifici procedimenti penali.

In particolare, al momento della stesura del secondo protocollo, si è pensato di sviluppare un meccanismo più snello per emettere ordini o richieste di produzione di informazioni sugli abbonati⁷⁶⁴ e sui dati di traffico⁷⁶⁵ ai fornitori di servizi aventi sede in altri Stati, perché i classici strumenti di cooperazione quali le richieste di assistenza reciproca per ottenere le prove elettroniche non sempre si rivelavano mezzi efficienti per trattare un numero crescente di richieste di prove elettroniche⁷⁶⁶. Possono mostrarsi utili ed interessanti ai fini investigativi e per il corretto svolgimento del procedimento penale anche le informazioni relative alle persone che registrano i domini, poiché molto spesso le forme di criminalità online sono facilitate da domini appositamente creati allo scopo o semplicemente sfruttati per obiettivi riprovevoli⁷⁶⁷. Pertanto, è stato ritenuto necessario sviluppare un quadro normativo efficiente per ottenere tali informazioni.

Durante la redazione del secondo protocollo, è stato affrontato anche il tema delle possibili attività da compiere in caso di situazioni di emergenza manifestabili quando vi è il rischio significativo ed imminente per la vita o la sicurezza di una persona fisica. In tali casi, appare necessaria un'azione rapida o prevedendo un'assistenza reciproca di emergenza o utilizzando i punti di contatto della Rete 24/7, istituita dalla Convenzione sulla criminalità informatica⁷⁶⁸.

dell'apertura per la firma del Secondo Protocollo addizionale in una delle loro prossime riunioni. Il testo sarà aperto alla firma a Strasburgo il 12 maggio 2022.

⁷⁶⁴ Tra le informazioni più ricercate figurano quelle relative all'abbonato e normalmente detenute dai fornitori di servizi, perché utili a identificare l'utente di una specifica e-mail o account di social media o di uno specifico indirizzo IP usato per la commissione del reato. Senza queste informazioni spesso è impossibile procedere a indagini penali internazionali relative alla criminalità informatica e ad altri crimini che coinvolgono le prove elettroniche. Si è appurato che ottenere informazioni sugli abbonati attraverso l'assistenza reciproca si è rivelato nella maggior parte dei casi inefficace. Alcune soluzioni sono state individuate con l'applicazione dell'art. 18 della Convenzione sulla criminalità informatica. Tuttavia, sono stati individuati ulteriori strumenti complementari per ottenere le informazioni sugli abbonati direttamente da un fornitore di servizi avente sede in un altro Stato.

⁷⁶⁵ Si ritiene che i dati di traffico siano spesso richiesti nelle indagini penali e la loro rapida divulgazione può essere necessaria per rintracciare la fonte di una comunicazione come punto di partenza per raccogliere ulteriori prove o per identificare un sospetto.

⁷⁶⁶ In tal senso, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 32.

⁷⁶⁷ Tali informazioni sono detenute da entità che forniscono servizi di registrazione di nomi di dominio, come i *registrars* e i *registries*. Il *registrar* è l'organizzazione autorizzata dal *registry* ad intervenire nel database del relativo *Top Level Domain* (TLD) (ad esempio .com, it., .net) e vendono nomi di dominio al pubblico; mentre il *registry* (Registro) o RNA è il Registro dei Nomi Assegnati, vale a dire il database dei nomi di dominio registrati sotto i vari TLD tenuto dalla *Registration Authority* competente, ossia l'organismo nazionale o internazionale responsabile di stabilire regole e procedure per l'assegnazione dei nomi di dominio e dell'assegnazione dei nomi di dominio, della gestione dei registri e dei *name server* primari dei vari TLD.

⁷⁶⁸ I redattori del secondo protocollo hanno anche approfondito altri strumenti di cooperazione internazionale come le videoconferenze e le squadre investigative comuni, già presenti nella Convenzione di assistenza giudiziaria in materia penale (ETS. n. 182) o in altri accordi bilaterali o multilaterali. Tuttavia, il protocollo mira a colmare solo alcune lacune. Nel corso delle discussioni, alcune misure non sono

Grazie anche al ruolo assunto dalla Commissione dell'Unione europea, si è ritenuto necessario prevedere, *inter alia*, una disciplina simile a quanto indicato all'art. 15 della Convenzione sulla criminalità informatica, funzionale a riconoscere che l'istituzione, l'attuazione e l'applicazione dei poteri e delle procedure relative alle indagini e ai procedimenti penali debbano sempre essere soggetti a condizioni e garanzie che assicurino un'adeguata protezione dei diritti umani e delle libertà fondamentali⁷⁶⁹.

In conclusione, gli argomenti e le sfide affrontate durante i lavori preparatori consentono di ritenere che il secondo protocollo apporti un valore aggiunto sia da una prospettiva operativa che politica, poiché potrà migliorare significativamente le capacità di cooperazione tra gli Stati e tra le Parti, i fornitori di servizi ed altri soggetti al fine di ottenere elementi elettronici dal valore investigativo e probatorio che possano rivelarsi utili nei procedimenti penali⁷⁷⁰.

Ancora una volta, sembra necessario approcciare al tema utilizzando il principio di ragionevolezza e di proporzionalità: da una parte si mira ad aumentare la capacità delle autorità di polizia di contrastare la criminalità, in generale, e quella informatica, in particolare; dall'altra, si presta particolare attenzione al pieno rispetto dei diritti umani e delle libertà fondamentali, sottolineando l'importanza ed il valore di uno spazio ove vi sia un libero flusso di informazioni, come deve essere internet.

8. Il Secondo protocollo alla Convenzione sulla criminalità informatica

Il Secondo protocollo alla Convenzione sulla criminalità informatica relativo alla cooperazione rafforzata ed alla divulgazione di prove elettroniche, così come indicato dall'art. 1, ha lo scopo di integrare la Convenzione tra le Parti del Secondo protocollo e di completare il Primo protocollo tra le Parti di esso che sono anche Parti del Secondo protocollo.

Come indicato nel Preambolo, l'esigenza di un Secondo protocollo nasce dalla consapevolezza che le prove di qualsiasi reato sono sempre più spesso conservate in forma elettronica su sistemi informatici collocati in giurisdizioni straniere, a volte

confluite nel secondo protocollo. Sebbene ritenute di grande interesse, a causa dei lavori supplementari che richiedevano dei tempi e delle ulteriori consultazioni necessarie, sia le indagini sotto copertura per mezzo di un sistema informatico sia l'estensione delle perquisizioni non sono stati ritenuti strumenti realizzabili nei tempi stabiliti per la preparazione del protocollo. Le parti si sono comunque riservate la possibilità di approntare tali strumenti con una fonte giuridica separata. Sul punto, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 33.

⁷⁶⁹ Tali garanzie di protezione dei dati integrano gli obblighi di molte delle Parti della Convenzione, che sono anche Parti della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (ETS n. 108). Il protocollo di modifica di tale Convenzione (ETS n. 223) è stato aperto alla firma durante la redazione del secondo protocollo nell'ottobre 2018. Va inoltre notato che il processo di redazione del presente protocollo comprendeva Parti all'epoca non vincolate agli strumenti del Consiglio d'Europa sulla protezione dei dati né alle norme dell'Unione europea in materia di protezione dei dati. Di conseguenza, sono stati compiuti sforzi significativi per garantire un protocollo equilibrato che rifletta i numerosi sistemi giuridici degli Stati che potrebbero essere Parti del protocollo, nel pieno rispetto delle garanzie poste a protezione della *privacy* e dei dati personali, come richiesto dalle Costituzioni e dagli obblighi internazionali di altre Parti della Convenzione. Sulla Convenzione n. 108, in relazione anche all'incapacità di colmare le lacune dell'art. 8 CEDU, M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, cit., p. 66 ss.

⁷⁷⁰ Così, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 33.

sconosciute. Per tale motivo, è necessario ottenere legalmente tali prove, al fine di consentire una risposta efficace della giustizia penale e per sostenere lo Stato di diritto.

Ebbene, su queste basi si è costruito un Protocollo che mira a rafforzare ulteriormente la cooperazione in materia di criminalità informatica e la capacità delle autorità giudiziarie penali di raccogliere elementi in forma elettronica dall'attitudine probatoria mediante: l'utilizzo di strumenti aggiuntivi più efficienti nonché di altre forme di cooperazione tra le autorità competenti; la cooperazione in situazioni di emergenza, ossia casi in cui c'è un rischio significativo e imminente per la vita o la sicurezza di qualsiasi persona fisica; e la cooperazione diretta tra le autorità competenti e i fornitori di servizi e altre entità che hanno il possesso o il controllo di informazioni pertinenti.

Per realizzare ciò, sembra che i redattori abbiano tentato teleologicamente di conseguire – secondo il principio personalista – un punto di equilibrio nei rapporti tra autorità e libertà⁷⁷¹, al fine di garantire, mediante bilanciamento, la protezione dei diritti umani e delle libertà fondamentali⁷⁷².

A tale conclusione si perviene analizzando quanto indicato nel Preambolo al Secondo protocollo, ove si evidenzia la consapevolezza della necessità di garantire che misure efficaci di giustizia penale sulla criminalità informatica e la raccolta di prove in forma elettronica siano soggette a condizioni e garanzie che prevedano l'adeguata protezione dei diritti umani e delle libertà fondamentali, compresi i diritti derivanti dagli obblighi che gli Stati hanno assunto in base agli strumenti internazionali applicabili in materia di diritti dell'uomo⁷⁷³.

⁷⁷¹ Sul rapporto tra "autorità" e "libertà", v., L. KALB, *Introduzione*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018, cit., p. 17 ss. Sul punto, si è anche osservato che l'epoca contemporanea ha visto la prevalenza del principio personalista. «Dopo l'esito infausto della concezione tradizionale della sovranità dello Stato, che ha dato base giuridica alle atrocità della prima metà del XX secolo, il ritorno delle libertà conculcate e dell'umanesimo negato ha imposto il rovesciamento del rapporto tra autorità e libertà». In particolare, oggi, l'assenza di limiti originari si riscontra nei diritti fondamentali enunciati dalle Costituzioni nazionali e dalle carte internazionali e sovranazionali. «Si parte dai diritti per arrivare allo Stato e non dallo Stato per arrivare ai diritti. Al fondamento di autorità del diritto si è sostituito il fondamento di valore. Per questo motivo l'invulnerabilità dei diritti fondamentali implica, come necessaria conseguenza giuridica, la irriducibilità *in pejus* delle norme costituzionali che li prevedono». Cfr., G. SILVESTRI, *L'individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018, cit., p. 21 ss. V., inoltre, P. CARETTI, *I diritti fondamentali. Libertà e diritti sociali*, II ed., Torino, 2005, p. 141 ss.

⁷⁷² Ad esempio, già nel Preambolo gli Stati membri del Consiglio d'Europa e gli altri Stati parti della Convenzione sulla criminalità informatica hanno riconosciuto che la raccolta di prove elettroniche per le indagini penali riguarda spesso dati personali, per cui è necessario proteggere la *privacy* e i dati personali per rispettare gli obblighi costituzionali e internazionali di molte Parti del Protocollo. In dottrina, si è osservato che l'evoluzione incessante dei mezzi tecnologici di controllo della vita privata, in tutte le sue manifestazioni, rende necessaria la tutela "progressiva" dei diritti fondamentali. In particolare, l'*iter* di perfezionamento della tutela della persona deve prevedere inevitabilmente un pieno e generale riconoscimento come diritto inviolabile della *privacy*. Così, G. SILVESTRI, *L'individuazione dei diritti della persona*, cit., p. 29. Sul punto, anche, R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. e proc. pen.*, 2014, p. 1133 ss.

⁷⁷³ Il riferimento è alla Convenzione per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali Convenzione del 1950 (STE n. 5) del Consiglio d'Europa, al Patto internazionale sui diritti civili e politici delle Nazioni Unite del 1966, alla Carta africana dei diritti dell'uomo e dei popoli del 1981, alla Convenzione americana sui diritti umani del 1969 e altri trattati internazionali sui diritti umani. Per un confronto tra la Convenzione di Strasburgo e la Carta di San José, v., A. DI STASI, *Il diritto all'equo processo nella CEDU e nella Convenzione americana sui diritti dell'uomo. Analogie, dissonanze e profili di convergenza giurisprudenziale*, Torino, 2012, p. 1-237, e spec. p. 27, secondo la quale «il sistema di protezione europeo dei diritti umani (identificato tradizionalmente con la CEDU) è assunto a modello per

Anche per il secondo protocollo si è deciso di fissare *standard* minimi di protezione che devono essere attuati da tutti gli Stati aderenti, lasciando aperta la possibilità per gli Stati più avanzati di prevedere tutele più forti per i loro cittadini. Tuttavia, tali *standard* di protezione più elevati non devono compromettere l'obiettivo comune della Convenzione e dei suoi protocolli, cioè rendere più efficiente ed efficace la cooperazione internazionale nella lotta contro la criminalità informatica⁷⁷⁴.

Strutturalmente, il Secondo protocollo è composta da 25 articoli suddivisi in quattro capitoli: I. Disposizioni comuni; II. Misure di cooperazione rafforzata; III. Condizioni e garanzie; IV. Disposizioni finali.

Il capitolo I contiene disposizioni comuni indicative dello scopo e dell'ambito di applicazione del Protocollo, nonché le definizioni della Convenzione applicabili al

lo sviluppo di sistemi paralleli quali quello interamericano (e quello africano, anch'esso in consistente processo di rafforzamento in senso giurisdizionale». Per una prospettiva comparatistica tra gli atti, si rinvia a, F. QUILLERE-MAJZOUB, *Le Protocole à la Charte africaine des droits de l'homme et des peuples relatif aux droits de la femme en Afrique: un projet trop ambitieux?*, in *RTDH*, 2007, p. 127 ss.; A. SACCUCCI, *Il Protocollo istitutivo della Corte africana dei diritti dell'uomo e dei popoli, un primo confronto con le altre Corti regionali*, in *Riv. Dir. int.*, 4, 2004, p. 1036 ss.; M. MUBIALA, *Contributions à l'étude comparative des mécanismes régionaux africain, américain et européen de protection des droits de l'homme*, in *Afr. J. Int. Comp. Law*, 9, 1997, p. 42 ss.; B. WESTON, R.A. LUKES, K. HNATT, *Regional Human Rights Regime. A Comparison and Appraisal*, in *Vanderbilt JTL*, 29, 1987, p. 587 ss.

⁷⁷⁴ In tal senso, si veda, ASSEMBLEA PARLAMENTARE COE, *Opinion 299(2021)* del 30 settembre 2021, par. 6, pubblicata al link: <https://pace.coe.int/pdf/4c2e2d5659bf8191941279e8e3e0782b1b7648ca03083ac61c80661120465d3e/opinion%20299.pdf>.

Protocollo e le ulteriori definizioni di termini utilizzati frequentemente⁷⁷⁵. Un ultimo articolo disciplina la lingua da usare per gli atti⁷⁷⁶.

⁷⁷⁵ L'art. 3 del Secondo protocollo, al par. 1 riprende le definizioni di cui agli articoli 1 e 18, par. 3, della Convenzione sulla criminalità informatica. Gli estensori hanno incluso queste definizioni perché questi termini sono utilizzati spesso nel testo e nella relazione esplicativa del Protocollo. Gli estensori hanno anche inteso che le spiegazioni fornite nella relazione esplicativa della Convenzione e nelle note orientative (adottate da T-CY) relative a tali termini si applicassero anche a tale Protocollo. Anche le definizioni dei reati e di altri termini inclusi nel testo della Convenzione sono destinate ad applicarsi ai fini della cooperazione tra le Parti del presente Protocollo, così come le definizioni dei reati e di altri termini utilizzati nel testo del Primo protocollo si applicano ai fini della cooperazione tra le Parti del Primo protocollo. Tuttavia, le Parti del Secondo protocollo che non sono parti del Primo protocollo non hanno l'obbligo di attenersi ai termini o alle definizioni stabilite nel Primo protocollo. Il par. 2 include ulteriori definizioni che si applicano al Protocollo: la lett. a) definisce l'“autorità centrale” come l'autorità o le autorità designate nell'ambito di un trattato o di un accordo di assistenza reciproca sulla base della legislazione uniforme o reciproca in vigore tra le Parti interessate o, in mancanza di questa, l'autorità o le autorità designate da una Parte ai sensi dell'art. 27, par. 2, lett. a) della Convenzione. Il Protocollo utilizza le autorità centrali in diversi articoli al fine di fornire una cooperazione attraverso un canale che le parti già usano e con cui hanno familiarità. Pertanto, le parti che hanno trattati di assistenza reciproca o accordi sulla base di una legislazione uniforme o reciproca sono tenute a utilizzare le autorità centrali designate ai sensi di tali trattati o accordi. Se non esiste alcun trattato o accordo di questo tipo tra le parti interessate, si applica la regola suppletiva, sussidiaria e non alternativa secondo cui le Parti sono tenute a utilizzare lo stesso canale delle autorità centrali che utilizzano attualmente ai sensi dell'art. 27, par. 2, lett. a), della Convenzione. Anche se non tutti i trattati di assistenza reciproca o accordi sulla base di una legislazione uniforme o reciproca utilizzano il termine “autorità centrale”, i redattori intendevano riferirsi alle autorità di coordinamento designate in tali trattati o accordi, comunque denominati. Inoltre, si riprende la definizione di autorità competente contenuta nelle Spiegazioni alla Convenzione sulla criminalità informatica, secondo cui si intende un'autorità giudiziaria, amministrativa o altra autorità incaricata dell'applicazione della legge che ha il potere, in base al diritto nazionale, di ordinare, autorizzare o intraprendere l'esecuzione di misure procedurali ai fini della raccolta o produzione di prove in relazione a specifiche indagini o procedimenti penali. Il par. 2 riporta anche la definizione di “emergenza” come una situazione in cui esiste un rischio significativo ed imminente per la vita o la sicurezza di qualsiasi persona fisica; la definizione di “dati personali” come informazioni relative a una persona fisica identificata o identificabile; e di “Parte trasferente” come la Parte che trasmette i dati in risposta a una richiesta o nell'ambito di una squadra investigativa comune o, ai fini del Capitolo II, Sezione 2, del Secondo protocollo, una Parte nel cui territorio si trova un fornitore di servizi di trasmissione o un ente che fornisce servizi di registrazione dei nomi di dominio. Infine, giova chiarire che nelle Spiegazioni al Protocollo, le Parti hanno inteso ritenere persona fisica identificabile quella che può essere identificata direttamente o indirettamente, con riferimento, in particolare, a un numero di identificazione o a uno o più elementi specifici della sua identità fisica, fisiologica, mentale, economica, culturale o sociale, mentre è considerato non identificabile quella persona nei cui confronti le attività di identificazione si rivelino onerose secondo fattori temporali, umani ed economici. Ciò se da un lato sembra che rappresenti un limite evidente alle attività investigative, dall'altro può essere di sicuro sprono alle Parti per lo sviluppo di tecnologie più efficienti, utili al raggiungimento di maggiori obiettivi. Tuttavia, proprio questo elemento disvela le profonde difficoltà relative alla formazione delle prove informatiche. Sul punto, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 35 ss.

⁷⁷⁶ L'art. 4 del Secondo protocollo tenta di rispondere ad un annoso problema verificatosi nella prassi, prevedendo un'ulteriore flessibilità ai sensi del Protocollo. Con una norma generale ed astratta, si fornisce un quadro delle lingue che possono essere utilizzate quando ci si rivolge alle Parti e ai fornitori di servizi o altre entità. In pratica, le Parti ben potrebbero essere in grado di lavorare in lingue diverse dalla loro lingua ufficiale, pur senza una specifica previsione del diritto nazionale o dei trattati. Tuttavia, spesso accade che le traduzioni inviate all'altro Stato siano imprecise o particolarmente onerose, con evidenti ripercussioni sul buon esito dell'assistenza giudiziaria. In particolare, i maggiori problemi si rinvergono nelle traduzioni da e verso le lingue meno comuni, poiché tali traduzioni possono rallentare le attività di assistenza giudiziaria o addirittura renderle impossibili a causa della loro scarsa qualità. Innanzi a tale situazione, alcuni Paesi non anglofoni avevano richiesto che l'inglese fosse inserito quale lingua obbligatoria nella compilazione delle richieste, poiché ritenuta particolarmente diffusa, soprattutto tra i principali fornitori di

Il capitolo II contiene i principali articoli del Protocollo che descrivono i vari metodi di cooperazione a disposizione delle Parti e rappresenta la parte più corposa dell'intero atto. Siccome a ciascun tipo di cooperazione si applicano principi diversi, è stato necessario suddividere il capitolo in cinque sezioni: Sezione 1 – Principi generali applicabili al capitolo II (art. 5); Sezione 2 – Procedure per migliorare la cooperazione diretta con fornitori ed entità di altre parti (artt. 6 e 7); Sezione 3 – Procedure per migliorare la cooperazione internazionale tra autorità per la divulgazione di dati informatici memorizzati (artt. 8 e 9); Sezione 4 – Procedure relative all'assistenza reciproca di emergenza (art. 10); Sezione 5 – Procedure relative alla cooperazione internazionale in assenza di accordi internazionali applicabili per la videoconferenza e per le attività delle squadre investigative comuni (artt. 11 e 12).

Il capitolo III indica condizioni e garanzie. In particolare, si richiede che le Parti applichino condizioni e garanzie simili all'art. 15 della Convenzione sulla criminalità informatica anche ai poteri e alle procedure di previste dal Secondo Protocollo. Inoltre, il capitolo include una serie dettagliata di garanzie per la protezione dei dati personali.

Le disposizioni finali contenute nel capitolo IV sono molto simili a quelle previste nei trattati del Consiglio d'Europa. Tra queste, vi sono alcune che estendono il campo di applicabilità delle disposizioni della Convenzione sulla criminalità informatica anche al Secondo protocollo. In particolare, l'art. 23 sulle "consultazioni delle Parti e valutazione dell'attuazione" rende applicabile l'art. 46 della Convenzione sulla criminalità informatica anche al Secondo protocollo e prevede che l'applicazione effettiva e l'attuazione delle disposizioni del protocollo siano valutati periodicamente dalle Parti. Tale previsione è utilissima al fine di aggiornare il protocollo in relazione agli sviluppi futuri delle nuove tecnologie.

L'articolo 2 pare confermare ciò che dovrebbe esser scontato, ma che, ad una attenta analisi, non è. L'ambito generale di applicazione del Protocollo è lo stesso di quello della Convenzione. In particolare, le misure contenute in tale Protocollo si applicano tra le Parti

servizi, e più semplice da tradurre rispetto a lingue poco diffuse. Diversamente, i redattori del Secondo protocollo hanno concluso che l'inglese non dovrebbe essere lingua obbligatoria nel Protocollo per una serie di motivi. Innanzitutto, alcuni Paesi condividono tra loro la stessa lingua ufficiale e, dunque, non hanno bisogno di utilizzare l'inglese; altri, invece, non hanno una classe di funzionari totalmente capace di leggere e comprendere l'inglese, pur essendo spesso coinvolta nelle richieste di assistenza. Pertanto, l'art. 4, par. 1, del Secondo protocollo richiede semplicemente che le richieste, gli ordini e le informazioni di accompagnamento siano redatte in una lingua accettabile per la Parte richiesta o notificata ai sensi dell'art. 7. La Parte può specificare la lingua accettabile anche se questa non è prevista nel suo diritto interno o nei trattati, aprendo, così, alla possibilità per alcuni Paesi di accettare richieste e ordini in lingue diverse e aggiuntive da quella specificata dal diritto interno o dai Trattati. La norma non interferisce con le disposizioni di quei trattati sull'assistenza reciproca che specificano la lingua o le lingue in cui devono essere presentate le richieste ai sensi di tali trattati. Mentre il par. 1 regola i rapporti linguistici tra Paesi, il par. 2 regola quelli tra Stato e fornitori di servizi o enti che forniscono servizi di registrazione di nomi di dominio sul territorio di un'altra Parte, ai fini degli artt. 6 e 7. Anche quest'ultima disposizione è volta a garantire una rapida cooperazione e una maggiore certezza nei rapporti, senza imporre nuovi ed eccessivi oneri ai privati che ricevono richieste o ordini. Le opzioni sono tre: la prima indica che l'ordine o la richiesta possono essere presentati in una lingua in cui il privato accetta abitualmente ordini o richieste nazionali da parte delle proprie autorità; la seconda prevede che se un fornitore di servizi o un ente accetta di ricevere ordini o richieste in un'altra lingua, questi possono essere presentati in quella lingua; la terza opzione consente allo Stato di emettere un ordine o una richiesta in una lingua diversa da quella accettata dal privato, purché accompagnati da una traduzione in una delle lingue accettate. Per rendere le procedure più efficienti, il T-CY si è impegnato ad adoperarsi informalmente per la raccolta di informazioni sulle lingue in cui gli ordini o le richieste e le informazioni di accompagnamento sono accettate dai privati. Per un approfondimento, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 37 ss.

del Protocollo, a specifiche indagini o procedimenti penali riguardanti i reati connessi a sistemi e dati informatici (ossia i reati di cui all'articolo 14 della convenzione, par. 2, lett. a e b), nonché alla raccolta di elementi in forma elettronica aventi attitudine probatoria di un reato (articolo 14 della Convenzione, par. 2 lett. c)⁷⁷⁷. Inoltre, il par. 1, lett. b) del Secondo protocollo stabilisce che le regole del protocollo si applicano tra le Parti del Primo protocollo che sono anche Parti del Secondo nell'ambito di specifiche indagini o procedimenti penali riguardanti i reati stabiliti ai sensi del Primo protocollo. Tuttavia, le Parti del Secondo protocollo che non sono parti del Primo non hanno l'obbligo di applicare quanto stabilito dal Secondo protocollo per i reati indicati nel Primo protocollo.

È evidente che ciascuna Parte è tenuta ad avere una base giuridica per adempiere agli obblighi stabiliti nel protocollo se i suoi trattati, leggi o accordi non contengono già tali disposizioni. Ciò non muta le disposizioni esplicitamente discrezionali in disposizioni obbligatorie, né modifica le disposizioni che permettono dichiarazioni o riserve. Come per la Convenzione, anche per il Protocollo è possibile che alcune Parti non abbiano necessità di alcuna legislazione di attuazione al fine di applicare le disposizioni del protocollo⁷⁷⁸.

9. Le procedure volte a migliorare la cooperazione diretta con fornitori ed enti privati di altre Parti. Elementi di comunanza

Nell'ambito delle misure di cooperazione rafforzata, viene disciplinata nello specifico la "cooperazione diretta", la quale permette alle autorità competenti di una Parte di collaborare direttamente con gli enti privati, al fine di raccogliere elementi aventi attitudine probatoria direttamente da enti che forniscono servizi di registrazione di nomi di dominio (art. 6) e dai fornitori di servizi (art. 7) in caso di specifiche indagini o processi penali⁷⁷⁹.

Si dovrebbe ritenere che le Parti reputino particolarmente importante disciplinare la cooperazione diretta con i privati, alla luce del forte slancio verso l'efficienza e l'efficacia delle indagini che essa realizza. A sostegno di tale tesi milita l'assetto strutturale del Secondo protocollo, il quale regola tale forma di cooperazione rafforzata prima di tutte le altre, con gli artt. 6 e 7.

Preliminarmente, va chiarito che ai sensi dell'art. 5, par. 2, del Secondo protocollo⁷⁸⁰, la disciplina relativa alla cooperazione diretta, così come descritta nella Sezione 2 del Capitolo II, si applica indipendentemente dall'esistenza o meno di un trattato di assistenza reciproca o un accordo sulla base di una legislazione uniforme o reciproca in vigore tra

⁷⁷⁷ Ciò significa che sia quando il reato è commesso mediante l'uso di un sistema informatico, sia quando un reato non commesso mediante un sistema informatico (ad esempio un omicidio) coinvolge prove elettroniche, possono essere utilizzati i poteri, le procedure e le misure di cooperazione previste dal protocollo.

⁷⁷⁸ Cfr., art. 2, par. 2 del Secondo protocollo alla Convenzione sulla criminalità informatica.

⁷⁷⁹ S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il secondo Protocollo addizionale alla Convenzione di Budapest*, cit., p. 1036 ss.

⁷⁸⁰ L'art. 5 del Secondo protocollo individua i principi generali applicabili al Capitolo II, chiarendo per ogni sezione se ed in che misura ogni singolo settore della cooperazione rafforzata è influenzato dall'esistenza di un Trattato o di un accordo di assistenza reciproca o altro tipo di legislazione tra le Parti interessate, come ad esempio gli accordi sulla base di una legislazione uniforme o reciproca sviluppati tra i Paesi nordici ed ammessi anche dalla Convenzione europea di assistenza giudiziaria in materia penale, e tra i Paesi del *Commonwealth*. Per il concetto di "accordo sulla base di una legislazione uniforme o reciproca", Cfr., *Explanatory Report to the Convention on Cybercrime*, par. 263, p. 47.

la Parte che richiede le informazioni e la Parte sul cui territorio si trova il privato che possiede o controlla tali informazioni.

I redattori hanno individuato due misure di cooperazione diretta: la richiesta di informazioni sulla registrazione del nome di dominio (art. 6) e la divulgazione di informazioni sugli abbonati (art. 7).

Entrambi gli strumenti sembrano essere un'evoluzione dell'ingiunzione di produrre, già disciplinato all'art. 18 della Convenzione sulla criminalità informatica, il quale, tuttavia, non rispondeva e non risponde alle attuali sfide poste dal sistema delle prove elettroniche, perché applicabile ad una serie limitata di casi. Invero, un evidente ostacolo all'applicazione dell'ingiunzione di produrre – come già osservato – è la circostanza per cui esso si può utilizzare quando un fornitore di servizi si trova nel territorio della Parte emittente ovvero offra ivi i suoi servizi⁷⁸¹.

Pertanto, le Parti del Secondo protocollo hanno considerato importante creare nuovi meccanismi complementari che permettano un accesso transfrontaliero diretto e, conseguentemente più efficace, alle informazioni elettroniche utili in un procedimento penale, arrivando alla creazione di strumenti che abbiano un campo di applicazione più ampio di quello individuato dall'ingiunzione di produrre.

I dati di base ottenibili attraverso tali strumenti non sono sufficienti a rivelare precise informazioni relative alla vita privata ed alle abitudini di vita quotidiana delle persone. Pertanto, siccome la divulgazione di tali dati può avere un grado di intrusività inferiore rispetto alla divulgazione di altre categorie di dati, si è ritenuto di poter procedere mediante una cooperazione diretta, consentendo di prevedere una disciplina che instauri un collegamento diretto tra una Parte ed un privato presente sul territorio di un altro Stato.

Tuttavia, l'attenzione verso i diritti fondamentali – in particolare, il diritto alla riservatezza – ha richiesto che gli strumenti avessero una struttura e limiti tali da non consentire richieste di produzioni di massa o dati in blocco⁷⁸².

Altra caratteristica comune è la possibilità per entrambi gli strumenti di utilizzare (oltre alle altre forme di comunicazione tradizionale) la forma elettronica, mediante l'utilizzo di apparecchi elettronici, per lo scambio di documenti e informazioni, quando ciò risulta accettabile per l'ente che fornisce il servizio. La *ratio* delle disposizioni previste all'art. 6, par. 4 e all'art. 7, par. 6 del Secondo protocollo – da considerare innanzitutto un incoraggiamento all'uso delle nuove tecnologie anche da parte delle autorità pubbliche di contrasto alla criminalità – risiede nel maggior livello di efficienza e velocità garantito dagli strumenti di comunicazione informatica.

⁷⁸¹ V., *supra*, Cap. III, par. 5.

⁷⁸² Di recente, anche la Corte europea dei diritti dell'uomo ha ribadito il principio per cui la sorveglianza di massa viola il diritto fondamentale alla vita privata ed alla *privacy* sancito all'art. 8 CEDU, nonché la libertà di espressione di cui all'art. 10 CEDU. Con la sent. Corte EDU, Grande Camera, 25 maggio 2021, *Big Brother Watch c. Regno Unito*, ricorsi nn. 58170/13 e 24960/15, la Corte ha stabilito che le intercettazioni preventive devono essere limitate a specifici sospetti ed essere oggetto di misure incisive di controllo. Secondo la Corte di Strasburgo, «i metodi di raccolta dei dati e la mole di persone tracciate non risultano specificati in maniera sufficiente e [...] mancano regole su filtraggio, ricerca e selezione delle comunicazioni sottoposte a controllo. [...] Raccogliere non solo i dati sul traffico ma anche il contenuto delle comunicazioni che possono essere monitorate costituisce una grave invasione della *privacy*. [...] Il sistema di sorveglianza di massa non è, di per sé, una violazione, ma tale sistema deve rispettare rigidi criteri [...]. Quanto attuato nel Regno Unito, invece, eccede il grado di interferenza che può essere considerato “necessario in una società democratica”». Per un primo commento alla sentenza, W. NOCERINO, *La sorveglianza di massa e i principi della CEDU*, in *Intelligence Security Investigation*, 28 giugno 2021, disponibile al link: <https://intelligencesecurityinvestigation.it/la-sorveglianza-di-massa-e-i-principi-della-cedu/>.

Di conseguenza, qualora sia ritenuto accettabile dall'ente che fornisce i servizi di registrazione dei nomi di dominio o dal *service provider*, l'autorità pubblica competente ai sensi dell'art. 3, par. 2, lett. b) del Secondo protocollo, può presentare una richiesta al privato in forma elettronica, utilizzando ad esempio una casella di posta elettronica, portali elettronici o altri mezzi informatici.

Tuttavia, appare necessario garantire la sicurezza, l'autenticità e la riservatezza delle comunicazioni. Invero, come previsto non solo per gli strumenti di cui all'art. 6 e 7, ma anche per l'ordine di produzione accelerata di informazioni sugli abbonati e dati sul traffico di cui all'art. 8 del Secondo protocollo, è necessario che la comunicazione in forma elettronica avvenga garantendo un livello appropriato di sicurezza tramite canali o mezzi sicuri per la comunicazione o utilizzando speciali scudi che proteggono soprattutto dagli attacchi informatici⁷⁸³.

9.1. *La procedura per l'ottenimento di informazioni sulla registrazione del nome di dominio*

Con l'art. 6 del Secondo protocollo, le Parti hanno convenuto di disciplinare una procedura che prevede la cooperazione diretta tra le autorità di uno Stato e un ente che fornisce servizi di registrazione di nomi di dominio sul territorio di un'altra Parte per ottenere informazioni sulle registrazioni degli *internet domain name*.

Uno dei passi principali di fondamentale importanza nei procedimenti penali e soprattutto nella fase delle indagini è costituito dall'ottenimento di dati relativi alla registrazione del nome di dominio. Tali dati si rivelano indispensabili per indirizzare le indagini su un preciso binario e per determinare con chiarezza l'autorità straniera con cui intrattenere rapporti di cooperazione internazionale nel caso concreto.

Siccome oggi i criminali si avvalgono sempre più spesso di domini per scopi riprovevoli e illeciti, l'accesso alle informazioni relative alla persona fisica o giuridica che ha registrato un dominio – il c.d. “*registrant*” – risulta fondamentale per identificare le persone fisiche che materialmente durante il procedimento penale potranno assumere lo *status* di persona sottoposta alle indagini e, successivamente, di imputato.

Per raggiungere l'obiettivo di ottenere informazioni per identificare o contattare il registrante di un nome di dominio in modo efficace ed efficiente, il Secondo protocollo introduce una procedura basata sulla richiesta di informazioni sulla registrazione del nome di dominio.

Orbene, il par. 1 e il par. 2 dell'art. 6 del Secondo protocollo sono speculari e disciplinano il primo, l'ipotesi in cui lo Stato sia parte attiva, qualora sia una sua autorità competente di emissione a richiedere le informazioni; il secondo, l'ipotesi in cui il privato situato nello Stato parte del protocollo debba rispondere ad una richiesta di informazioni sulla registrazione del nome di dominio.

Nello specifico, le Parti si impegnano a adottare le misure necessarie per consentire alle proprie autorità competenti di rivolgere le richieste direttamente ad un ente che

⁷⁸³ Si ritiene che possano rivelarsi necessari i metodi di autenticazione. Si potrebbe operare utilizzando una varietà di mezzi o una loro combinazione che permetta una sicura identificazione dell'autorità richiedente. Ad esempio, i mezzi possono includere una conferma dell'autenticità tramite una nota dell'autorità della Parte emittente (come un'autorità centrale o un'altra autorità designata), comunicazioni successive tra l'autorità emittente e la Parte ricevente, la tecnica delle cifrature, l'uso di un indirizzo e-mail ufficiale, o altri mezzi tecnologicamente avanzati che progressivamente in futuro saranno inventati ed implementabili. Sul punto, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 51.

fornisce servizi di registrazione di nomi di dominio nel territorio dell'altra Parte, senza l'intervento mediato dell'altro Stato, nonché a individuare misure che consentano agli enti privati presenti sul proprio territorio che forniscono servizi di registrazione di nomi di dominio di divulgare le informazioni in risposta alle richieste provenienti da altri Stati.

La relazione esplicativa chiarisce che è concessa ampia flessibilità agli Stati nell'individuazione del formato delle richieste, le quali possono adattarsi alle peculiarità giuridiche e politiche dei singoli ordinamenti. Invero, le Parti possono utilizzare lo schema dell'ordine, che, tuttavia, verrà trattato in ogni caso come una richiesta non vincolante, non potendo incidere sulla natura volontaria di tale forma di cooperazione, così come regolata dall'art. 6 del Secondo protocollo⁷⁸⁴.

Innanzitutto, l'art. 6 del Secondo protocollo non pone alcun obbligo in capo agli enti privati di rispondere positivamente ad ogni richiesta, lasciandole in capo una valutazione discrezionale pilotata dai principi garantistici indicati dall'atto stesso.

In particolare, per facilitare la cooperazione, la norma richiede alle Parti una base giuridica chiara a cui rifarsi, l'individuazione di autorità competenti aventi il potere di formulare richieste, il presupposto dell'utilità delle informazioni ai fini delle indagini o, più in generale, di un procedimento penale, una dichiarazione che attesti la necessità delle informazioni poiché rilevanti ai fini di un procedimento penale e l'uso esclusivo delle informazioni per specifiche indagini o uno specifico procedimento penale ben individuato, ai sensi dell'art. 6, par. 3, lett. c) del Secondo protocollo. Sono, inoltre, previste specifiche garanzie per il trattamento dei dati personali divulgati e trasferiti a seguito di tali richieste attraverso l'art. 14 del Secondo protocollo⁷⁸⁵.

Le informazioni – richiedibili solo ai fini di un procedimento penale specifico – devono essere in possesso o sotto il controllo dell'ente privato e devono essere finalizzate a identificare o contattare il registrante di un nome di dominio. Pertanto, si tratterebbe di dati quali le generalità, l'indirizzo fisico, l'indirizzo e-mail e il numero di telefono di un *registrant* che non permettono di trarre precise conclusioni relative alla vita privata ed alle abitudini quotidiane delle persone. Di conseguenza, ciò consente un rapporto diretto tra l'autorità competente e l'ente privato nel pieno rispetto del diritto alla *privacy* degli individui.

Per quanto attiene al contenuto minimo, la richiesta deve includere la data della richiesta, l'identità e le informazioni di contatto dell'autorità competente che emette la richiesta; il nome di dominio in merito al quale si richiedono le informazioni e un elenco dettagliato delle informazioni richieste, compresi gli specifici elementi di dati come il nome, l'indirizzo fisico, l'indirizzo e-mail o il numero di telefono, una dichiarazione che la richiesta è formulata ai sensi del Secondo protocollo ed è conforme ad esso, con la quale la Parte conferma che le informazioni sono necessarie perché rilevanti ai fini di

⁷⁸⁴ La formulazione dell'art. 6, par. 1, del Secondo protocollo è sufficientemente ampia da poter ritenere che le richieste e le informazioni possono essere ottenute utilizzando portali internet, interfacce informatiche o altri strumenti tecnologici funzionali a facilitare o accelerare la divulgazione delle informazioni richieste. In tal senso, v., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 43.

⁷⁸⁵ Per facilitare la cooperazione, la relazione esplicativa consente anche al privato di cooperare alla luce di accordi contrattuali stipulati con l'ICANN (*Internet Corporation for Assigned Names and Numbers*), l'ente di gestione internazionale degli incarichi relativi alla rete internet, istituito nel 1998. Di primaria importanza è il suo ruolo nell'assegnazione degli indirizzi IP e di identificatore di protocollo e di gestione del sistema dei nomi di dominio di primo livello (*Top-Level Domain*) generico (gTLD), del codice internazionale (ccTLD) e dei sistemi di *root server*. Per un approfondimento, si visiti il sito internet dell'ente all'indirizzo web: <https://www.icann.org/>.

indagini penali e, più in generale, di un procedimento penale e che le informazioni saranno utilizzate solo per quella specifica indagine o procedimento penale⁷⁸⁶, i tempi e le modalità di divulgazione delle informazioni, nonché qualsiasi altra speciale istruzione procedimentale, come può essere una richiesta di riservatezza, o una richiesta di non divulgazione della richiesta al dichiarante o a terzi, al fine di evitare, ad esempio, una prematura *discovery*.

Al fine di tutelare i diritti della persona nei cui confronti si richiedono i dati e, nell'equilibrio tra autorità e libertà, per preservare la segretezza delle indagini penali, il contenuto minimo della richiesta non prevede un'esposizione – neanche sommaria – dei fatti. Tuttavia, l'ente privato potrebbe essere interessato ad ottenere delle informazioni ulteriori relative al fatto non solo per valutare la richiesta, ma anche per meglio adempiere ad essa. Pertanto, la relazione esplicativa consente all'ente privato di richiedere informazioni, qualora sia indispensabile per l'esecuzione della richiesta⁷⁸⁷.

Alla richiesta preventiva di informazioni relative al fatto formulata dal privato, si affianca un'altra forma di dialogo pubblico/privato prevista dal paragrafo 5, finalizzata al miglioramento dei rapporti tra l'autorità competente e l'ente, attivabile in caso di rifiuto della richiesta. Invero, lo Stato potrebbe richiedere all'ente di indicare i motivi di rifiuto alla base del diniego della divulgazione delle informazioni ovvero avviare una consultazione con la Parte in cui ha sede l'ente, al fine di individuare le misure disponibili per ottenere le informazioni⁷⁸⁸.

La *ratio* si rinviene nell'essenza dello strumento della richiesta, strumento non vincolante per le Parti. In un'ottica di maggior collaborazione e per rendere gli strumenti di cooperazione giudiziaria in materia penale più efficienti, le Parti hanno deciso di creare strumenti di confronto dialettico che possano rappresentare le vere chiavi di volta per la risoluzione di conflitti relativi all'esecuzione delle richieste.

9.2. La divulgazione delle informazioni sugli abbonati

Qualora un'autorità competente volesse ottenere direttamente da un fornitore di servizi informazioni relative agli abbonati, dovrà attivare lo strumento previsto all'art. 7 del Secondo Protocollo⁷⁸⁹.

⁷⁸⁶ In particolare, risulta evidente che per i Paesi europei, per informazioni necessarie debbano intendersi quelle specifiche informazioni necessarie e proporzionate secondo quanto indicato dai principi della Convenzione per la salvaguardia dei diritti dell'Uomo e delle Libertà Fondamentali, così come interpretati dalla Corte europea dei diritti dell'Uomo, nonché dalla legislazione e dalla giurisprudenza nazionale. Diversamente, per le altre Parti si dovranno applicare i principi correlati al loro ordinamento, come i principi di pertinenza. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 45.

⁷⁸⁷ Sul punto, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 45.

⁷⁸⁸ Il paragrafo 6 richiede che ciascuna Parte, al momento della firma al Protocollo o del deposito dello strumento di ratifica, accettazione o approvazione, o in qualsiasi altro momento, comunichi al Segretario Generale del Consiglio d'Europa l'autorità designata che funga da punto di contatto per le consultazioni previste dal paragrafo 5 del Secondo protocollo. È inoltre prevista l'istituzione e l'aggiornamento ad opera del Segretario Generale di un registro delle autorità designate dalle Parti ai sensi del paragrafo 6.

⁷⁸⁹ Tuttavia, l'art. 7, par. 9, prevede la possibilità per una Parte – al momento della firma del protocollo o del deposito del suo strumento di ratifica, accettazione o approvazione – di riservarsi il diritto di non applicare lo strumento o di vietare l'applicazione dello stesso nelle ipotesi in cui la divulgazione di alcuni tipi di numeri di accesso risultasse lesiva dei principi fondamentali del proprio ordinamento.

Le informazioni ottenibili mediante ordine sono le stesse di quelle definite all'art. 18, par. 3, della Convenzione sulla criminalità informatica consistenti in qualsiasi informazione contenuta sottoforma di dato informatico o qualsiasi altra forma detenuta da un *internet service provider*, relativa agli abbonati, diversa dai dati di traffico o di contenuto⁷⁹⁰.

È bene precisare che l'ordine di divulgazione si presenta come uno strumento più evoluto rispetto all'ingiunzione a produrre prevista dall'art. 18 della Convenzione sulla criminalità informatica. Invero, i redattori erano ben consapevoli dei limiti dell'ingiunzione, pertanto hanno sviluppato un sistema di cooperazione diretta che dovrebbe essere più flessibile ed efficiente, poiché instaura un rapporto più saldo – basato su regole chiare e precise – tra autorità pubblica e fornitori di servizi stabiliti nel territorio di un'altra parte. Tuttavia, non dovrebbe essere pregiudicata la capacità delle Parti di eseguire gli ordini emessi ai sensi dell'art. 18 della Convenzione sulla criminalità informatica, né la possibilità di accedere a forme di cooperazione volontaria.

L'ordine deve avere ad oggetto informazioni specifiche e memorizzate sugli abbonati e va presentato a un fornitore di servizi stanziato fisicamente sul territorio di un'altra Parte⁷⁹¹. Presupposti sono: il possesso o il controllo dei dati da parte del *service provider*; la necessità delle informazioni per l'indagine o il procedimento penale indicato⁷⁹²; il divieto di richieste di produzioni di massa o dati in blocco⁷⁹³. Quale condizione, è richiesto che le informazioni debbano essere utilizzate esclusivamente per specifiche indagini o procedimenti penali.

L'art. 7 del Secondo protocollo, dunque, obbliga le parti a adottare tutte le misure legislative e organizzative necessarie per consentire alle proprie autorità competenti di

⁷⁹⁰ Nello specifico, si tratterebbe di informazioni relative a: il tipo di servizio di comunicazione utilizzato; le disposizioni tecniche prese a tale riguardo e il periodo del servizio; l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio; ogni altra forma di informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio. Le informazioni necessarie per identificare l'abbonato di un servizio possono essere relative anche agli indirizzi IP. Per l'elenco delle informazioni ottenibili, si rinvia all'*Explanatory Report to the Convention on Cybercrime*, par. 177-183, p. 30 ss.

⁷⁹¹ È escluso che il semplice fatto che un fornitore di servizi abbia un rapporto contrattuale con una società presente sul territorio di un altro Stato, senza la presenza fisica su di esso del fornitore, consenta di ritenere che il fornitore di servizi sia stanziato sul territorio di quella Parte. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 48.

⁷⁹² È stato chiarito che per i Paesi che hanno aderito alla Convenzione europea per la salvaguardia dei diritti dell'Uomo e delle Libertà Fondamentali del 1950 le informazioni devono essere necessarie e proporzionate, secondo quanto stabilito dalla Convenzione stessa, così come interpretata dalla Corte europea dei diritti dell'uomo, nel pieno rispetto della legislazione e giurisprudenza nazionale. Le altre Parti applicano, invece, il principio di pertinenza, evitando ordini che prevedano una divulgazione di informazioni troppo ampia. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 47 ss.

⁷⁹³ Tuttavia, in controtendenza rispetto agli arresti del passato, nella giurisprudenza dell'Unione europea è stata sancita la legittimità della conservazione indifferenziata e generalizzata dei dati personali. Cfr., Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, causa C-623/17, *Privacy International*; Corte di giustizia, Grande sezione, sentenza del 6 ottobre 2020, causa C-511/18, *La Quadrature du Net*. Per un commento alle sentenze, M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, cit., p. 93 ss.

emettere tali ordini e ai fornitori di servizi presenti sul proprio territorio di divulgare le informazioni richieste sugli abbonati, in risposta agli ordini.

Siccome tra i vari sistemi giuridici vi sono differenze anche profonde, la formulazione dei primi due paragrafi è tale da consentire agli Stati di attuare misure diverse per stabilire una procedura che permetta alla cooperazione diretta di essere quanto più efficace ed efficiente. È stato chiarito che gli ordinamenti possono sia eliminare semplicemente gli ostacoli giuridici posti ai fornitori di servizi per rispondere a un ordine, fornendo una base giuridica solida su cui calibrare le proprie decisioni, sia obbligare i fornitori di servizi a rispondere agli ordini in determinate ipotesi⁷⁹⁴.

Ciò che non deve mancare è la garanzia da parte degli Stati che i fornitori di servizi ottemperino agli ordini nel rispetto delle regole, formulate in modo da salvaguardare la certezza del diritto, evitando responsabilità giuridiche in capo agli *internet service providers* conformatisi in buona fede agli ordini emessi da un altro Stato.

Data la delicatezza delle informazioni richieste e dello strumento realizzato, l'art. 7, par. 2, lett. b), del Secondo protocollo, consente alle Parti contraenti di inserire un ulteriore elemento di garanzia, dichiarando, al momento del deposito del proprio strumento di ratifica, accettazione o approvazione, che l'ordine impartito ai fornitori di servizi stanziati sul proprio territorio debba essere emesso da – o sotto il controllo di – un ufficio di un pubblico ministro o da un'altra autorità giudiziaria o altrimenti essere emesso sotto il controllo di un'autorità indipendente.

Per l'ordine è previsto un contenuto minimo obbligatorio ed uno supplementare, che può essere incluso nel modello dell'ordine, se consentito dalla legge, o essere allegato e fornito separatamente. Sia l'ordine, sia le informazioni supplementari devono essere trasmessi direttamente al fornitore di servizi.

L'ordine dovrà includere le informazioni relative all'autorità di emissione e la data di emissione; le informazioni che identificano il fornitore di servizi; il reato oggetto dell'indagine o del procedimento penale; l'autorità che richiede le informazioni sull'abbonato⁷⁹⁵; una descrizione dettagliata delle specifiche informazioni richieste sull'abbonato. L'ordine deve, inoltre, contenere una dichiarazione che l'ordine è emesso ai sensi del Secondo protocollo, così da attestarne la conformità al protocollo⁷⁹⁶.

Non è prevista alcuna descrizione dei fatti, poiché le indagini restano pur sempre segrete. Inoltre, tale attività comporterebbe una *discovery* nei confronti di un privato, non ritenuta accettabile secondo i principi dettati dal Consiglio d'Europa, perché lesiva dei diritti fondamentali della persona.

L'autorità emittente potrebbe, però, anche scegliere di includere ulteriori informazioni per agevolare il trattamento o perché richiesto dal proprio diritto interno. Ai sensi dell'art. 7, par. 4, del Secondo protocollo, si tratta di dati relativi: ai motivi giuridici interni che autorizzano l'autorità a emettere l'ordine; alle disposizioni legali e alle sanzioni

⁷⁹⁴ Tuttavia, dovrebbe residuare in capo ai fornitori di servizi una responsabilità per motivi diversi dal rispetto dell'ordine, come ad esempio, l'inosservanza di un requisito giuridico applicabile o di uno standard di sicurezza delle informazioni memorizzate. In tal senso, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 48.

⁷⁹⁵ In alcuni Stati, l'autorità di emissione e l'autorità che richiede i dati potrebbero non identificarsi con lo stesso soggetto. Ad esempio, l'ufficio del pubblico ministero potrebbe essere l'autorità che richiede i dati, mentre l'autorità di emissione potrebbe coincidere con il giudice che autorizza ed emette l'ordine. Pertanto, è previsto in tali casi l'indicazione di entrambe le autorità.

⁷⁹⁶ Così, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 49.

applicabili per il reato oggetto dell'indagine o del procedimento penale; ai contatti dell'autorità alla quale il fornitore di servizi deve inviare le informazioni sull'abbonato, richiedere ulteriori informazioni o rispondere; ai tempi e ai modi in cui inviare le informazioni richieste.

Inoltre, i dati possono far riferimento ad altri procedimenti avviati per la conservazione dei dati informatici, compresa la data di conservazione e i numeri di riferimento; alla dichiarazione dell'esecuzione di una notifica simultanea avvenuta ai sensi del paragrafo 5; a qualsiasi altra informazione che possa aiutare ad ottenere l'invio delle informazioni sull'abbonato e ad eventuali istruzioni procedurali speciali⁷⁹⁷. Deve ritenersi che l'autorità non sia comunque tenuta ad inviare tutte le informazioni supplementari, ma potrebbe determinarsi per l'invio anche solo di una o alcune di esse.

Nell'ipotesi in cui un fornitore di servizi rifiuti l'invio dei dati sull'abbonato o ometta di rispondere entro il termine di trenta giorni ovvero nel diverso termine indicato nelle informazioni aggiuntive, ai sensi dell'art. 7, par. 7, del Secondo protocollo, l'autorità di emissione può attivare la procedura prevista per l'ordine di produzione accelerata, di cui all'art. 8 del Secondo protocollo o altre forme di assistenza reciproca, con una procedura semplificata di conversione dell'ordine, al fine di accelerare i tempi di esecuzione dello strumento.

Per l'attivazione degli strumenti surrogatori, sembrerebbe necessario che il fornitore di servizi indichi i motivi di rifiuto, in modo tale da ridurre il margine di errore nelle procedure o semplicemente interrompere le operazioni di cooperazione, qualora i dati non siano più disponibili.

Accanto alla parte obbligatoria, vi sono ulteriori istituti che possono essere previsti per l'applicazione dello strumento. In particolare, al momento della firma del protocollo o con il deposito dello strumento di ratifica, accettazione o approvazione, e in qualsiasi altro momento, uno Stato può notificare al Segretario generale del Consiglio d'Europa l'adozione delle regole per l'esecuzione della notifica simultanea, per lo svolgimento delle consultazioni tra le autorità nonché per l'applicazione del divieto di divulgazione da parte di un'autorità designata⁷⁹⁸.

Con l'istituto della notifica simultanea, uno Stato chiede che, nell'emettere un ordine indirizzato ad un fornitore di servizi, – in tutti i casi ovvero in determinate circostanze espressamente individuate – l'autorità di emissione esegua una notifica simultanea dell'ordine, delle informazioni supplementari e di una breve descrizione dei fatti relativi all'indagine o al procedimento all'autorità designata.

⁷⁹⁷ Tra le istruzioni procedurali speciali si annoverano le richieste di riservatezza e le richieste di autenticazione. La richiesta di riservatezza può prevedere, ad esempio, il divieto di divulgazione dell'ordine all'abbonato o ad altre parti, qualora non impediscano al fornitore di consultare le autorità da notificare ai sensi del paragrafo 5a) o consultate ai sensi del paragrafo 5b). Qualora la riservatezza sia volta ad evitare una divulgazione prematura dei fatti, va indicato nella richiesta. Va sottolineato che in alcuni Stati la riservatezza dell'ordine è mantenuta in applicazione della legge, a differenza di altri in cui potrebbe non esservi alcuna disciplina. Le istruzioni procedurali speciali possono anche prevedere l'indicazione del canale di trasmissione più adatto alle esigenze dell'autorità di emissione. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 49 ss.

⁷⁹⁸ Ai sensi dell'art. 7, par. 5, lett. e) del Secondo protocollo, nei casi in cui sia prevista l'esecuzione della notifica simultanea, lo svolgimento delle consultazioni tra le autorità, l'applicazione del divieto di divulgazione da parte di un'autorità designata e delle ulteriori attività di cui all'art. 7, par. 5, lett. d), lo Stato designi un'unica autorità, da comunicare al Segretario generale del Consiglio d'Europa, insieme con le informazioni di contatto. Il Segretariato del Consiglio d'Europa è tenuto a istituire e mantenere un registro delle autorità designate e delle circostanze in cui è richiesta la notifica simultanea.

Indipendentemente dall'adesione alle regole relative alla notifica simultanea, una Parte può richiedere che si attuino le regole relative all'istituto della consultazione tra autorità previste dall'art. 7, par. 5, lett. b), prima che si inviino le informazioni all'autorità di emissione, solo in determinate circostanze.

La limitazione a soli specifici casi appare essere frutto di un compromesso, per evitare che in ogni caso si potesse causare un ritardo significativo nella produzione dei dati richiesti, con serio rischio per il buon esito delle indagini o del procedimento penale. Pertanto, si è previsto che la consultazione sia possibile solo in specifici casi come, ad esempio, il dubbio che vi siano elementi per ritenere la sussistenza di un motivo di rifiuto o che possa verificarsi un serio pregiudizio per le indagini o per i procedimenti penali della Parte trasferente.

In ogni caso, sia la procedura di notifica, sia la procedura di consultazione appaiono totalmente discrezionali, non essendo previsto un obbligo di richiedere l'una o l'altra procedura⁷⁹⁹.

Le autorità notificate o consultate, senza indebito ritardo, possono opporre un divieto di divulgazione delle informazioni qualora ravvisino un pregiudizio per le indagini o per i procedimenti penali nel proprio Stato o nel caso in cui si realizzino i motivi di rifiuto quali una richiesta avente come presupposto un reato politico o connesso o recante un pregiudizio alla sovranità, alla sicurezza, all'ordine pubblico ad altri interessi essenziali dello Stato o nel caso di ulteriori motivi di rifiuto previsti dalla legislazione interna o dai trattati di mutua assistenza applicabili⁸⁰⁰. Qualora l'autorità emetta un divieto di divulgazione nei confronti di un fornitore di servizi, ai sensi dell'art. 7, par. 5, lett. d), n. II, deve informare prontamente l'autorità alla quale il fornitore di servizi avrebbe dovuto inviare i dati sull'abbonato dell'emissione del divieto di divulgazione e dei contestuali motivi che hanno indotto l'autorità ad emetterlo.

Ai fini dell'emissione di un divieto di divulgazione, l'autorità notificata o consultata può anche chiedere all'autorità alla quale il fornitore di servizi dovrebbe inviare i dati sull'abbonato le informazioni supplementari di cui all'art. 7, par. 4, del Secondo protocollo, senza rivelarle al fornitore di servizi presente sul proprio territorio.

Al momento della firma del protocollo ovvero del deposito dello strumento di ratifica, accettazione o approvazione, uno Stato può dichiarare di voler prevedere come prioritario lo strumento dell'ordine di divulgazione delle informazioni sugli abbonati di cui all'art. 7, rispetto all'ordine di produzione accelerata di cui all'art. 8 del Secondo protocollo, a meno che la Parte emittente fornisca una spiegazione ragionevole per cui non ritiene di dover attivare lo strumento di cui all'art. 7 del Secondo protocollo in via prioritaria.

Con tale dichiarazione, si crea un binario preferenziale per lo strumento dell'ordine di divulgazione, mentre la procedura di cui all'art. 8 verrebbe attivata soltanto nelle ipotesi in cui non abbia avuto successo la procedura di cooperazione diretta di cui all'art. 7.

⁷⁹⁹ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 50.

⁸⁰⁰ Il chiaro rimando è all'art. 25, par. 4 e all'art. 27, par. 4 della Convenzione sulla criminalità informatica.

10. Le nuove procedure di cooperazione internazionale tra autorità per la produzione di dati informatici

Accanto agli strumenti di cooperazione diretta con i privati, gli Stati firmatari del Secondo protocollo alla Convenzione sulla criminalità informatica hanno sviluppato sistemi di cooperazione internazionale tra autorità straniere per la ricerca e la formazione di prove elettroniche più efficienti rispetto a quelli già esistenti.

Seppur basato sul principio della mutua assistenza, la disciplina prevista alla Sezione III del Secondo protocollo mira a migliorare la cooperazione internazionale tra autorità straniere compiendo un enorme passo evolutivo: non più il rigido e farraginoso schema previsto solitamente per gli strumenti basati sul principio di mutua assistenza, ma robusta apertura a forme di cooperazione basate su una fiducia reciproca più forte e salda, partendo dal presupposto che una seria lotta alla criminalità informatica – più veloce e subdola rispetto agli altri tipi – debba strutturarsi prevedendo un sistema rogatorio caratterizzato da concretezza e velocità delle operazioni, senza rinunciare alle garanzie previste per i diritti fondamentali⁸⁰¹.

Pertanto, ancora una volta, si assiste ad una delicata opera di bilanciamento dei diritti e degli interessi in gioco, secondo i principi di ragionevolezza e proporzionalità⁸⁰², o – come affermato da rilevante dottrina – secondo il principio della “ragionevolezza della proporzione”⁸⁰³.

A differenza degli artt. 6 e 7 del Secondo protocollo, i quali prevedono un rapporto tra autorità di una Parte e privato con sede nel territorio di un altro Stato, gli strumenti previsti dagli artt. 8 e 9 del Secondo protocollo si basano su un rapporto diretto tra autorità straniere perché con essi si va a caccia di informazioni più sensibili. Con l’aumento del rischio di ledere i diritti fondamentali, le Parti hanno previsto un innalzamento delle garanzie.

In questa operazione, si potrebbe teorizzare l’esistenza – e la conseguente applicazione – del principio della “gradualità degli strumenti rogatori”, secondo cui all’aumentare della sensibilità delle informazioni richieste, devono aumentare le garanzie

⁸⁰¹ Il Preambolo al Secondo protocollo sulla criminalità informatica chiarisce che l’attenzione per una migliore cooperazione giudiziaria tra autorità nasce dall’esigenza di combattere la crescente minaccia per la democrazia, lo Stato di diritto ed i diritti umani ad opera di un uso criminale delle tecnologie di informazione e comunicazione. Con la crescita della criminalità informatica, si amplia anche la platea di vittime, per cui è stato necessario individuare un valido compromesso, rappresentato dal punto di equilibrio tra gli interessi contrapposti.

⁸⁰² In dottrina è stato osservato che nella formazione delle prove elettroniche si assiste a un paradosso nel rapporto tra rispetto dei diritti fondamentali e il principio di proporzionalità: se si vuole garantire l’affidabilità del materiale digitale, si rischia di violare il diritto alla privacy; se si vuole proteggere al meglio il diritto alla privacy, si rischia di perdere quote di affidabilità. In tal senso, A. CAMON, *The project devices and digital evidence in Europe*, cit., p. 9.

⁸⁰³ Per questa espressione, G. SILVESTRI, *L’individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018, cit., p. 30 ss. Secondo l’A., «da qualche tempo trova sempre maggiore ascolto la tendenza teorica a far riferimento al criterio di proporzionalità, da preferire a quello di ragionevolezza, sulla scia della giurisprudenza del Tribunale costituzionale tedesco e delle Corti europee. Non condivido l’entusiasmo per questa sostituzione. Se la proporzione fosse rigorosamente numerica, si tratterebbe di un criterio più preciso di quello, indeterminato, della ragionevolezza, i cui risultati sono sempre opinabili. Ma non è così. Stabilire se due entità sono tra loro in rapporto di proporzionalità involve una serie di valutazioni e giudizi di valore, che difficilmente consentono di ricavare un risultato certo. [...] In definitiva, a mio modesto avviso, proporzionalità e ragionevolezza sono termini pressoché sinonimi. L’uso del primo serve tuttavia, sul piano retorico, ad accreditare una pretesa natura “oggettiva” del bilanciamento».

predisposte a tutela dei diritti fondamentali, prevedendo uno strumento diverso. Conseguenza è la previsione di strumenti “a più velocità”, alcuni caratterizzati da una maggior celerità, altri da maggior lentezza.

Gli strumenti di maggior impatto sui diritti fondamentali e sulla sfera del singolo sembrano siano comunque ridotti ad *extrema ratio*, non potendo indicare specifici mezzi di compensazione della lesione dei diritti fondamentali in gioco. È, anche in questo caso, l'applicazione del principio di proporzionalità e della legalità processuale.

Tuttavia, rispetto agli strumenti previsti nella Convenzione sulla criminalità informatica, è stata sviluppata una procedura più veloce ed efficiente, ritenuta necessaria per affrontare le nuove sfide presentatesi a causa di una criminalità informatica sempre più imperante.

Va necessariamente chiarito che, come per gli strumenti di cooperazione diretta con i fornitori ed enti privati stabiliti sul territorio di altre Parti, anche gli strumenti di cooperazione internazionale tra autorità straniere previste dal Secondo protocollo non si sostituiscono, ma si affiancano a quelli già disciplinati con la Convenzione sulla criminalità informatica⁸⁰⁴.

Per cui, le Parti sono libere di scegliere lo strumento ritenuto più adeguato al caso concreto, in base a proprie valutazioni discrezionali, e decidere, tra l'altro, di attivare in caso di emergenza gli strumenti ritenuti idonei.

Si tratta, in astratto, di prevedere, ed in concreto, di scegliere lo strumento più idoneo, meno afflittivo e che rechi il minor pregiudizio possibile alla sfera individuale, con il minor sacrificio necessario ai diritti fondamentali, mediante una valutazione prognostica di successo.

In particolare, gli artt. 8 e 9 del Secondo protocollo implementano due strumenti aggiuntivi che garantirebbero una maggiore efficienza dell'assistenza reciproca tra le autorità competenti⁸⁰⁵.

L'evoluzione è epocale e comporta un radicale mutamento delle usuali regole della mutua assistenza. Con i nuovi strumenti, ciò che nel classico sistema di mutua assistenza era regola, sembra tramutarsi in eccezione, ciò che era eccezione si trasforma in regola.

Tuttavia, la penetrante disciplina di riserve e condizioni a cui possono aderire le Parti rischia di minare l'efficienza dei moderni strumenti.

Oltre a ciò, si sottolinea l'assenza di disposizioni che disciplinano le modalità di raccolta, analisi e presentazione del materiale informatico, al fine di garantirne l'attendibilità⁸⁰⁶.

Sullo sfondo, resta l'obiettivo dichiarato e da raggiungere: migliorare la capacità degli Stati di reagire contro la criminalità transfrontaliera, anche di matrice informatica, con

⁸⁰⁴ Come chiarito dall'art. 5, par. 7, del Secondo protocollo, anche questi strumenti non pregiudicano la cooperazione – compresa quella spontanea – tra Stati o tra Stati e fornitori di servizi attuabile mediante altri accordi, intese, pratiche o diritto interno.

⁸⁰⁵ Cfr., Preambolo al Secondo protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione di prove elettroniche.

⁸⁰⁶ Su tale aspetto, in riferimento a tutti i progetti relativi alla ricerca e formazione delle prove elettroniche, v., A. CAMON, *The project devices and digital evidence in Europe*, cit., p. 4 ss., secondo il quale la problematica non è stata affrontata perché frutto di un malinteso che ritiene gli elementi elettronici aventi attitudine probatoria oggettivamente affidabili. Tuttavia, gli elementi informatici sono portatori di una serie di paradossi perché se da un lato, i dati informatici sono molto facili da trasferire – generando così la forte esigenza di una regolamentazione legale uniforme –, dall'altro, la disciplina internazionale è fondata su principi ed evita disposizioni specifiche. Sebbene attraversare le frontiere per svolgere un'indagine digitale oggi è molto semplice attraverso il ricorso ai nuovi meccanismi di assistenza giudiziaria, le procedure restano rigide, lente, sproporzionate.

strumenti tecnologicamente più avanzati, alla luce delle evoluzioni politiche e sociali in Europa. I progressi tecnologici intervenuti a livello mondiale hanno costretto gli Stati a rivedere i propri sistemi rogatoriali, rendendo più agevole, più rapida e più flessibile l'assistenza reciproca, con l'abbandono di schemi vetusti e farraginosi, proteggendo al contempo i diritti fondamentali.

Partendo da tale assunto, si è ritenuto di sviluppare anche strumenti idonei a produrre elementi informatici in caso di emergenza. In particolari casi, come in ipotesi di rischio significativo e imminente per la vita o la sicurezza di una persona fisica, è necessario ottenere rapidamente i dati informatici. Pertanto, i redattori hanno ritenuto di dover trovare un nuovo equilibrio tra gli interessi e i diritti fondamentali, creando strumenti – come quello previsto all'art. 9 del Secondo protocollo – da attivare in occasioni particolarmente eccezionali, ove rilevi la tutela del diritto alla vita ed alla sicurezza delle persone fisiche.

Ancora una volta, il Consiglio d'Europa ha agito con la massima attenzione verso i diritti fondamentali, ritenendo che nessun diritto sia “tiranno” sull'altro, ed individuando, seppur generalmente ed astrattamente, ipotesi particolari in cui gli equilibri “si spostano” talora a favore di uno, talaltra a favore di un altro diritto fondamentale.

10.1. *L'ordine di produzione accelerata*

L'art. 8 del Secondo protocollo disciplina il nuovo istituto dell'ordine di produzione accelerata di informazioni sugli abbonati e di dati sul traffico⁸⁰⁷. Si tratta di uno strumento che coinvolge direttamente le autorità straniere, e solo indirettamente i fornitori di servizi stanziati sul territorio di uno Stato richiesto.

Gli Stati sono incoraggiati alla massima flessibilità possibile per la presentazione di richieste basate su tale strumento, ma possono – al momento della firma del protocollo o del deposito del suo strumento di ratifica, accettazione o approvazione – dichiarare che la richiesta sia presentata da un'autorità centrale o da un'altra autorità individuata di comune accordo tra le Parti interessate⁸⁰⁸.

Con tale strumento, uno Stato emette un ordine di produzione da presentare nell'ambito di una richiesta a un altro Stato. Lo Stato richiesto ha la possibilità di dare esecuzione a tale ordine, obbligando un fornitore di servizi presente sul suo territorio⁸⁰⁹ a produrre le informazioni sugli abbonati ovvero i dati sul traffico in possesso o sotto il controllo del fornitore di servizi, necessari per specifiche indagini o per uno specifico processo penale. Anche per tale strumento, dalle informazioni sugli abbonati sono esclusi i dati relativi al contenuto.

Si tratta di un meccanismo di integrazione delle disposizioni di assistenza reciproca. Invero, lo strumento dell'ordine di produzione accelerata integra e non sostituisce le procedure di assistenza reciproca già previste dalla Convenzione sulla criminalità

⁸⁰⁷ Ai sensi dell'art. 8, par. 13, del Secondo protocollo, al momento della firma del protocollo o del deposito del suo strumento di ratifica, accettazione o approvazione, uno Stato può riservarsi il diritto di non applicare lo strumento alla produzione dei dati di traffico.

⁸⁰⁸ V., art. 8, par. 11, del Secondo protocollo.

⁸⁰⁹ È richiesta la presenza fisica sul territorio dello Stato di esecuzione, non essendo sufficiente la sola esistenza di un rapporto contrattuale tra il fornitore di servizi non presente fisicamente sul territorio dello Stato richiesto e una società presente sul territorio dello Stato richiesto. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 53.

informatica ovvero dagli altri accordi multilaterali o bilaterali⁸¹⁰, proponendo uno schema di cooperazione giudiziaria di tipo rogatorio più snello e rapido rispetto ai sistemi precedenti⁸¹¹.

Per tale procedura, è stato previsto il modello dell'ordine, sostanziato in qualsiasi procedimento legale che obbliga un fornitore di servizi a divulgare al richiedente le informazioni sugli abbonati o i dati sul traffico. L'ordine può assumere sia la forma dell'ordine di produzione sia un altro meccanismo autorizzato dalla legge che può essere emesso allo scopo di obbligare il privato a produrre le informazioni richieste⁸¹².

Al fine di facilitare la trasmissione delle informazioni, dei dati e dei documenti, lo Stato richiesto è tenuto ad accettare le richieste in forma elettronica. Tuttavia, può richiedere l'uso di mezzi di comunicazione elettronica sicuri e che garantiscano l'autenticazione, prima di accettare la richiesta⁸¹³.

Per obbligare un fornitore di servizi a cedere le informazioni e i dati richiesti, è necessario che gli Stati adottino le misure legislative o di altro tipo ritenute più adeguate a rendere esecutivo l'ordine⁸¹⁴.

L'ordine di produzione accelerata è uno strumento più lento rispetto all'ordine di divulgazione delle informazioni sugli abbonati, perché non prevede un rapporto diretto tra autorità straniera e *internet service provider* stabilito sul territorio di un altro Stato, ma al contempo – date le maggiori garanzie che offre – consente di richiedere non solo informazioni relative agli abbonati ma anche dati sul traffico, ritenute informazioni maggiormente sensibili, e per questo ottenibili solo con uno strumento che tuteli maggiormente i diritti fondamentali.

L'attenzione ai diritti fondamentali ed al delicato equilibrio tra autorità e libertà è così forte da aver spinto i redattori del protocollo ad inserire una clausola di riserva, secondo cui gli Stati possono decidere di non applicare l'ordine di produzione accelerata ai dati sul traffico. Controbilanciamento a tale scelta è rappresentato dal divieto per gli Stati che aderiscono a tale riserva di inviare ordini di produzione accelerata ad altri Stati per l'ottenimento di dati dello stesso tipo⁸¹⁵.

L'ordine di produzione accelerata deve contenere le informazioni fondamentali per l'esecuzione, le informazioni di supporto e le eventuali istruzioni procedurali speciali.

⁸¹⁰ In effetti, nel caso in cui sia necessario richiedere contemporaneamente le informazioni sugli abbonati, i dati sul traffico e i dati sul contenuto, può risultare più efficiente optare per un unico strumento rogatorio tradizionale, anziché cercare di ottenere alcuni dati utilizzando l'ordine di produzione accelerata ed altri attraverso una richiesta di assistenza giudiziaria separata. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 53.

⁸¹¹ Cfr., S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il secondo Protocollo addizionale alla Convenzione di Budapest*, cit., p. 1037.

⁸¹² Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 53.

⁸¹³ V., art. 8, par. 5, del Secondo protocollo.

⁸¹⁴ L'*Explanatory report* chiarisce che le Parti possono dare esecutività ad un ordine di un altro Stato, riconoscendo l'ordine come equivalente ad un provvedimento nazionale o emettendo un ordine di produzione interno, purché siano rispettati i diritti costituzionalmente previsti ed i diritti umani. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 53 ss.

⁸¹⁵ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 58.

Le informazioni fondamentali per l'esecuzione sono rivelabili anche al fornitore di servizio richiesto dei dati e rappresentano il cuore dell'ordine⁸¹⁶.

Le informazioni di supporto, invece, sono ad uso esclusivo dello Stato richiesto e non sono condivise con i fornitori di servizi senza il consenso dello Stato richiedente, perché soggette al segreto investigativo⁸¹⁷. Si tratta di informazioni aggiuntive utili allo Stato richiesto per la decisione relativa all'esecuzione dell'ordine⁸¹⁸. Stabiliscono le basi giuridiche nazionali ed internazionali che consentono l'emissione dell'ordine nonché informazioni allo Stato richiesto necessarie per valutare l'esistenza di motivi di rifiuto o condizioni da applicare⁸¹⁹.

Oltre alle informazioni tassativamente richieste ai sensi del par. 3, lett. b), con l'art. 8, par. 4, del Secondo protocollo le Parti hanno stabilito che è consentito agli Stati – al momento della firma del protocollo o del deposito del suo strumento di ratifica, accettazione o approvazione, e in qualsiasi altro momento – di dichiarare la volontà di ricevere ulteriori informazioni di supporto, necessarie per dare esecuzione all'ordine⁸²⁰. Si tratterebbe di informazioni supplementari, richieste dal diritto interno, che integrano ulteriori requisiti ritenuti necessari per ottenere la produzione dei dati elettronici. Inoltre, lo Stato richiesto può chiedere chiarimenti in merito alle informazioni già fornite ai sensi dell'art. 8, par. 3, lett. b) del Secondo protocollo.

Le istruzioni procedurali speciali – come, ad esempio, le richieste di certificazione o di riservatezza della richiesta ovvero la compilazione dei moduli di autenticazione degli elementi aventi attitudine probatoria – assicurano il corretto trattamento della richiesta e, pertanto, vanno indicate al momento della trasmissione dell'ordine. Lo Stato richiesto, in aggiunta, può indicare al fornitore di servizi delle informazioni supplementari, come le

⁸¹⁶ Si tratta delle informazioni relative all'autorità di emissione e alla data di emissione dell'ordine; alla dichiarazione di conformità dell'ordine all'art. 8 del Secondo protocollo; al nome e all'indirizzo del o dei fornitori di servizi da notificare; al reato o reati che costituiscono oggetto dell'indagine o del processo penale; all'autorità che richiede le informazioni o i dati, se diversa dall'autorità di emissione; alla descrizione dettagliata delle informazioni o dei dati specifici richiesti. In particolare, l'autorità che richiede le informazioni o i dati potrebbe essere, ad esempio, un'autorità inquirente; mentre l'autorità di emissione potrebbe essere un giudice.

⁸¹⁷ Già al momento dell'invio dell'ordine, gli Stati dovrebbero indicare se le informazioni di supporto possono essere condivise con il fornitore di servizi.

⁸¹⁸ Nello specifico, l'art. 8, par. 3, lett. b) del Secondo protocollo, indica tra le informazioni di supporto la base legale che autorizza l'autorità all'emissione di un ordine di produzione; le disposizioni che individuano la fattispecie astratta di reato per cui si procede e la relativa gamma di sanzioni; tutte le informazioni che la Parte richiedente può fornire e che consentono di concludere che il fornitore o i fornitori di servizi sono in possesso o controllano le informazioni o i dati richiesti; un breve riassunto dei fatti relativi all'indagine o al processo penale; una dichiarazione che attesti la rilevanza delle informazioni o dei dati per l'indagine o il processo penale per cui si richiedono gli elementi elettronici; le informazioni di contatto di una o più autorità nel caso in cui l'autorità competente dello Stato richiesto avesse necessità di richiedere ulteriori informazioni per l'esecuzione dell'ordine; notizie relative all'eventuale conservazione delle informazioni o dei dati già richiesti, che possono permettere allo Stato richiesto di confrontare la richiesta con le precedenti richieste di conservazione, facilitando la divulgazione delle informazioni o dei dati originariamente conservati; indicazioni relative a eventuali informazioni o dati già ricercati e dei mezzi utilizzati, nel caso in cui lo Stato richiedente abbia già chiesto informazioni sugli abbonati o dati sul traffico direttamente al fornitore di servizi.

⁸¹⁹ In tal senso, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 54.

⁸²⁰ Le informazioni di supporto "aggiuntive" vanno tassativamente specificate al momento della firma del protocollo o del deposito del suo strumento di ratifica, accettazione o approvazione, e in qualsiasi altro momento. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 56.

modalità di produzione o l'indicazione dell'autorità a cui devono essere divulgati i dati nello Stato richiesto.

Una volta ricevuto l'ordine, nonché tutti i documenti e le informazioni necessarie, lo Stato richiesto deve adottare tutte le misure ragionevoli per procedere rapidamente all'esecuzione della richiesta. Seppur sia l'art. 8, par. 6 del Secondo protocollo, sia l'*Explanatory report* richiedano i «*reasonable efforts*», non vi è alcun documento che specifichi cosa si debba intendere per sforzi ragionevoli né su quali parametri bisognerebbe valutare la ragionevolezza.

Gli sforzi ragionevoli sono richiesti soltanto in relazione alle attività sotto il diretto controllo delle autorità pubbliche. Non sono richiesti, invece, per i fornitori di servizi, in quanto privati. Invero, sembra sia stato demandato al singolo Stato l'individuazione di mezzi che obblighino gli *internet service providers* a produrre gli elementi elettronici il più rapidamente possibile, pur nella consapevolezza che potrebbero sussistere molti fattori che rischiano di ritardarne la produzione⁸²¹.

Tuttavia, sono individuati i termini di esecuzione della richiesta. Invero, in assenza di motivi di rifiuto e di rinvii di esecuzione, e dopo l'eventuale dialogo tra autorità sulle eventuali condizioni di esecuzione, la Parte richiesta deve trattare e notificare la richiesta al fornitore di servizi entro 45 giorni. Deve, inoltre, obbligare il fornitore di servizi a produrre entro 20 giorni le informazioni sugli abbonati ed entro 45 giorni i dati sul traffico.

I parr. 7, 8 e 9 aprono ad un delicato sistema di dialogo tra autorità, al fine di rendere flessibile la procedura di cui all'art. 8, consentendo – per quanto possibile – l'esecuzione dell'ordine.

In particolare, qualora lo Stato richiesto non possa ottemperare alle istruzioni procedurali speciali, deve avviare un dialogo con lo Stato richiedente, informandolo prontamente dell'impossibilità di eseguire quanto indicato e specificando, se del caso, eventuali condizioni a cui potrebbe conformarsi. Spetterà alla Parte richiedente ritirare l'ordine ovvero informare lo Stato richiesto di proseguire nell'esecuzione della richiesta, nei limiti indicati⁸²².

Il par. 8, invece, regola i motivi di rifiuto, il rinvio dell'esecuzione e le condizioni di esecuzione. In particolare, per quanto attiene ai motivi di rifiuto, il paragrafo rimanda a quelli indicati all'art. 25, par. 4 e all'art. 27, par. 4 della Convenzione sulla criminalità informatica⁸²³. La Parte richiesta può decidere anche di rinviare l'esecuzione nel caso in cui questa possa recare pregiudizio per le indagini o per i processi penali condotti dalle proprie autorità. Infine, lo Stato richiesto può anche decidere di condizionare la richiesta ricevuta.

La Parte richiesta notifica alla Parte richiedente la sua decisione di rifiutare, condizionare o rinviare l'esecuzione della richiesta ovvero le circostanze che potrebbero ritardare l'esecuzione della richiesta in modo significativo. Inoltre, la Parte richiesta può applicare una clausola di limitazione d'uso degli elementi informatici, condizionando la

⁸²¹ Tra i fattori di rischio si annoverano: le opposizioni dei fornitori di servizi o la loro assenza di risposte, il mancato rispetto della data di restituzione degli elementi elettronici, il volume delle richieste da trattare. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 56.

⁸²² V., art. 8, par. 7, del Secondo protocollo.

⁸²³ Nello specifico, si tratta dei casi in cui una richiesta abbia quale presupposto un reato politico o connesso o recante un pregiudizio alla sovranità, alla sicurezza, all'ordine pubblico ad altri interessi essenziali dello Stato o nel caso di ulteriori motivi di rifiuto previsti dalla legislazione interna o dai trattati di mutua assistenza applicabili.

comunicazione delle informazioni all'esplicito divieto di farne uso per indagini o procedimenti diversi da quelli indicati nella richiesta⁸²⁴.

Il dialogo tra autorità diventa particolarmente importante nel caso di apposizione di condizioni all'esecuzione della richiesta, perché l'art. 8, par. 9 del Secondo protocollo dispone che qualora lo Stato richiedente non ritenga di poter accettare le condizioni comunicate dallo Stato richiesto ai sensi del par. 8, ne deve dare prontamente comunicazione, in modo da consentire alla Parte richiesta di decidere se fornire le informazioni richieste con l'ordine anche senza il rispetto delle condizioni apposte.

Se, però, la Parte richiedente accetta la condizione, ne è vincolata e lo Stato richiesto che fornisce le informazioni sotto condizione può chiedere spiegazioni sull'uso fatto degli elementi informatici e del materiale inviato.

In relazione al dialogo tra autorità, si assiste ad un sistema fluido ed elastico, perché aperto alla discrezionalità delle Parti che possono individuare un punto di convergenza mediante un confronto dialettico, al fine di consentire l'esecuzione dell'ordine, raggiungendo l'obiettivo. Tuttavia, la costellazione di deroghe, condizioni e riserve possibili sembrano irrigidire il procedimento anziché semplificarlo. Le autorità saranno sempre costrette a verificare cosa sia richiesto dagli altri Stati, per non commettere errori ed evitando motivi di rifiuto o lungaggini procedurali che impediscono l'esecuzione della richiesta e, di conseguenza, l'acquisizione degli elementi informatici aventi attitudine probatoria.

Orbene, un punto di equilibrio, che tenterà di evitare la stasi o il rallentamento della procedura, potrebbe essere il portale in cui confluiranno tutte le indicazioni relative alle informazioni di contatto delle autorità designate, alle riserve ed alle deroghe opposte da ciascuno stato. Tuttavia, sarà necessario rendere facilmente accessibile ed utilizzabile la piattaforma.

10.2. *La divulgazione accelerata di dati informatici in assenza di una richiesta di assistenza*

L'art. 9 del Secondo protocollo disciplina uno strumento basato sul principio della massima cooperazione accelerata, che risponde ai requisiti della rapidità e dell'efficienza. Si tratta di una procedura volta ad ottenere dati informatici utilizzando la Rete 24/7, senza una preventiva richiesta di assistenza reciproca⁸²⁵, in casi di emergenza, caratterizzati dal pericolo significativo ed imminente per la vita o la sicurezza di qualsiasi persona fisica, come, ad esempio, in caso di attacchi terroristici o attacchi *ransomware* che possono paralizzare un sistema ospedaliero⁸²⁶ ovvero quando si indaga sugli *account* di posta

⁸²⁴ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 56 ss.

⁸²⁵ Tuttavia, ai sensi dell'art. 9, par. 5, del Secondo protocollo, al momento della firma del protocollo o del deposito del proprio strumento di ratifica, accettazione o approvazione, uno Stato può dichiarare di voler ottenere, dopo l'esecuzione della richiesta, una successiva richiesta di assistenza reciproca, la quale può fungere da formale documentazione della richiesta di emergenza, nonché informazioni supplementari.

⁸²⁶ Nel corso della pandemia da Covid-19 si sono verificati importanti attacchi anche alle strutture sanitarie e di ricerca scientifica. Ad esempio, a settembre 2020, l'ospedale universitario di Düsseldorf, in Germania è stato vittima di un *ransomware* che ha criptato i dati e bloccato tutti i sistemi informatici. A seguito di tale evento, si è reso indispensabile trasferire in altre cliniche pazienti gravi – tra cui una donna deceduta durante il tragitto – e posticipare interventi chirurgici urgenti. Anche l'ospedale universitario di Brno, in Repubblica Ceca e l'ospedale Spallanzani di Roma sono stati vittime di attacchi informatici. A ciò va aggiunto un elevato numero di aziende private, che spesso non godono di un numero sufficiente di esperti di sicurezza informatica e soffrono difficoltà economiche dovute al sostenimento di costi di aggiornamento

elettronica utilizzati dai sequestratori di persona per comunicare con i familiari delle vittime al fine di ottenere un riscatto⁸²⁷.

Vero protagonista della procedura è la Rete 24/7, disciplinato all'art. 35 della Convenzione sulla criminalità informatica⁸²⁸ che, con i suoi punti di contatto, si rende disponibile per facilitare l'esecuzione delle richieste di divulgazione accelerata di dati provenienti dagli Stati in caso di emergenza.

La Rete 24/7 risulta particolarmente adatta alle attività da svolgere in caso di emergenza perché riesce a ridurre i tempi per l'ottenimento delle informazioni elettroniche, in caso di richieste urgenti e ad alta priorità, stringendo al massimo i tempi della procedura.

Invero, la Rete 24/7 è composta da punti di contatto che riescono a comunicare rapidamente tra loro e senza bisogno di traduzioni, riuscendo così a soddisfare le richieste ricevute da altri Stati, sia rivolgendosi direttamente ai fornitori di servizi presenti sul territorio, sia sollecitando altre autorità competenti, sia comunicando direttamente con le autorità giudiziarie, quando previsto dal diritto interno di uno Stato⁸²⁹.

Lo schema previsto dall'art. 9 del Secondo protocollo – che richiede agli Stati di adottare le misure legislative e di altro tipo necessarie – è particolarmente semplice: il punto di contatto di uno Stato richiede immediata assistenza al fine di ottenere la divulgazione dei dati informatici ad un punto di contatto di un'altra Parte; il punto di contatto richiesto chiederà i dati al fornitore di servizi con sede sul proprio territorio; il fornitore di servizi rivela all'autorità richiesta i dati informatici; l'autorità dello Stato richiesto fornisce i dati allo Stato richiedente. Il punto di contatto della Rete 24/7 nello Stato richiedente opera, dunque, come canale per trasmettere la richiesta al punto di contatto della Rete 24/7 dell'altro Stato.

La formulazione è così generale da consentire un'ampia discrezione in capo agli Stati nel determinare i requisiti per l'applicazione dello strumento previsto all'art. 9 del Secondo protocollo. Margini di manovra sono lasciati anche nella scelta sia di meccanismi alternativi maggiormente idonei a soddisfare la Parte richiedente sia dell'autorità più adatta ad eseguire una richiesta pervenuta da un punto di contatto⁸³⁰.

dei sistemi di sicurezza. Europol ha inoltre registrato un significativo aumento anche di pedopornografia, ludopatie compulsive, attività di disinformazione, truffe e frodi negli acquisti online. Va, infine, sottolineato come dal rapporto del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), nel 2020, nonostante siano raddoppiati gli attacchi informatici ed aumentato il numero di indagini avviate, le richieste di cooperazione internazionale in ambito della Rete 24/7 siano 65, in diminuzione rispetto al 2019, in cui furono 74. Le statistiche sono consultabili al link: <https://www.commissariatodips.it/notizie/articolo/cnaipic-e-tempo-di-bilancio-relativo-all-anno-2020/index.html>. Intanto, solo nel periodo gennaio-marzo 2021 l'Osservatorio cybersecurity di Exprivia ha attestato un aumento del 47% dei crimini informatici rispetto al 2020 in Italia.

⁸²⁷ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 58.

⁸²⁸ Invero, ai sensi dell'art. 35 della Convenzione sulla criminalità informatica include, tra le forme di assistenza prestata dalla Rete 24/7, la facilitazione, o se il diritto interno di uno Stato o la prassi nazionale lo consentono, l'applicazione diretta di misure volte alla ricerca di elementi aventi attitudine probatoria e la trasmissione di informazioni dal carattere giuridico e localizzazione dei sospetti.

⁸²⁹ Inoltre, i punti di contatto, essendo centri di prossimità, possono anche consigliare gli Stati richiedenti su questioni relative ai fornitori di servizi o alla ricerca di elementi informatici aventi attitudine probatoria, spiegando la disciplina nazionale da rispettare per ottenere la divulgazione dei dati. In tal modo, si migliora la comunicazione e la comprensione degli istituti vigenti nei singoli Stati.

⁸³⁰ Cfr., Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 60.

Risultato che vuole raggiungere il procedimento è la divulgazione rapida di specifici dati informatici memorizzati⁸³¹, detenuti dai fornitori di servizi sul territorio del punto di contatto richiesto. L'ampiezza terminologica utilizzata indicherebbe quanto sia ritenuto importante ottenere non solo le informazioni sugli abbonati, ma anche contenuti memorizzati e dati sul traffico, in situazioni di emergenza, in cui si possa prescindere dal presupposto della necessaria presentazione di una formale richiesta di assistenza reciproca⁸³². In particolare, i dati in oggetto sono memorizzati o esistenti e non comprendono dati che non sono ancora venuti ad esistenza, come i dati sul traffico o sul contenuto relativi a future comunicazioni⁸³³.

Presupposti per l'ottenimento dei dati informatici richiesti mediante la procedura prevista all'art. 9 sono lo stato di emergenza, la memorizzazione o l'esistenza dei dati informatici prima dell'attivazione della procedura, il possesso o il controllo dei dati da parte del fornitore di servizi, l'esistenza di una indagine o di un processo penale in cui i dati si rivelano utili. Non è necessaria una preventiva richiesta di assistenza reciproca, poiché i punti di contatto devono avere la capacità di trasmettere e ricevere le richieste ai sensi dell'art. 9 in caso di emergenza, senza la compilazione anticipata del modello.

Le informazioni da fornire con tale richiesta sono destinate a facilitare l'esame e, se del caso, l'esecuzione della richiesta da parte dell'autorità competente dello Stato richiesto⁸³⁴. Lo Stato richiesto potrebbe avere la necessità di ottenere ulteriori chiarimenti sulla richiesta o informazioni supplementari per l'esecuzione. In tal caso, le consultazioni dovrebbero avvenire con il punto di contatto della Parte richiedente. Inoltre, la richiesta deve essere accettata anche in forma elettronica⁸³⁵ e può essere accettata anche se trasmessa oralmente, con successiva richiesta di conferma in forma elettronica.

⁸³¹ Va precisato che, a differenza degli altri strumenti previsti dal Secondo protocollo, l'art. 9 non utilizza una terminologia stringente come "informazioni specifiche e memorizzate dall'abbonato", ma usa un'espressione più ampia quale "specifici dati informatici memorizzati". La terminologia coprirebbe qualsiasi dato informatico specificato, ossia qualsiasi fatto, informazione o concetto in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione, così come definito all'art. 1, par. 1, lett. b, della Convenzione sulla criminalità informatica.

⁸³² Tuttavia, merita particolare attenzione l'art. 9, par. 1, lett. b), del Secondo protocollo, il quale, in applicazione del principio di economicità e nel pieno rispetto delle garanzie previste per i diritti fondamentali, consente alla Parte di dichiarare di non voler eseguire le richieste che riguardino la sola divulgazione delle informazioni sugli abbonati. Invero, per alcune Parti, ricevere richieste unicamente per le informazioni sugli abbonati rischierebbe di sovraccaricare i punti di contatto di lavoro superfluo. Infatti, la stessa richiesta può ottenere un positivo riscontro utilizzando lo strumento dedicato per la divulgazione delle informazioni sugli abbonati di cui all'art. 7 ovvero l'ordine di produzione accelerata di cui all'art. 8 del Secondo protocollo, che consentono in ogni caso una rapida divulgazione delle informazioni. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 59.

⁸³³ Sul punto, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 59.

⁸³⁴ La richiesta deve contenere l'indicazione dell'autorità competente che richiede i dati e la data di emissione della richiesta, l'indicazione che la richiesta è formulata ai sensi dell'art. 9 del Secondo protocollo, il nome e l'indirizzo del fornitore o dei fornitori di servizi che possiedono o controllano i dati richiesti, l'indicazione del reato o dei reati oggetto d'indagine o del processo penale e un riferimento alle proprie disposizioni legali ed alle sanzioni applicabili, l'esposizione dei fatti sufficienti a dimostrare che sussiste il presupposto dell'emergenza e come i dati richiesti siano riconducibili a essa, la descrizione dettagliata dei dati richiesti, l'indicazione delle eventuali istruzioni procedurali speciali e qualsiasi altra informazione che possa aiutare ad ottenere la divulgazione dei dati richiesti.

⁸³⁵ Quando è utilizzata tale forma, possono essere richiesti livelli adeguati di sicurezza e di autenticazione.

La Parte richiesta non è tenuta a fornire i dati richiesti. Infatti, potrebbero esservi situazioni in cui gli Stati non forniscono i dati informatici perché ritengono che le stesse informazioni possano essere ottenute anche attraverso altri strumenti più appropriati. Se si verifica tale circostanza, l'art. 9, par. 6, del Secondo protocollo obbliga lo Stato richiesto ad informare in tempi rapidi la Parte richiedente i motivi di non esecuzione.

Tuttavia, è possibile instaurare un dialogo tra Parti, perché contestualmente alla comunicazione dei motivi di non esecuzione, potrebbe specificare le condizioni alle quali fornirebbe i dati e qualsiasi altra forma di cooperazione disponibile, al fine di raggiungere l'obiettivo di accelerare la divulgazione dei dati in caso di emergenza. In tal caso, se la Parte richiesta può soddisfare le condizioni, si vincolerà ad esse⁸³⁶ e l'esecuzione avverrà nel rispetto di quanto imposto; in caso contrario, la Parte comunicherà la propria impossibilità a soddisfare le condizioni indicate dallo Stato richiesto, il quale potrà decidere se le informazioni o il materiale debbano comunque essere forniti⁸³⁷.

Evidenti i vantaggi: tempi di procedura particolarmente ridotti; miglioramento dei rapporti e della fiducia reciproca tra gli Stati; facile autenticazione degli elementi aventi attitudine probatoria ottenute attraverso l'assistenza reciproca.

La compilazione, traduzione e trasmissione di una richiesta di assistenza reciproca mediante i canali tradizionali richiede tempi particolarmente lunghi, anche a causa del coinvolgimento delle autorità centrali, con eventuali ulteriori rallentamenti in caso di richieste di informazioni supplementari in forma scritta. La Rete 24/7, invece, opera in tempo reale, scambiando informazioni pressoché nell'immediato⁸³⁸. L'uso del canale creato con la Rete 24/7 può avere enormi vantaggi, anche rispetto ai principi previsti per l'assistenza reciproca di emergenza di cui all'art. 10 del Secondo protocollo. Uno di questi è la possibilità di evitare la preparazione di una richiesta di assistenza reciproca in anticipo.

11. La mutua assistenza d'emergenza

L'art. 10 del Secondo protocollo indica i principi generali e le regole integrative utilizzabili ed applicabili agli strumenti di assistenza giudiziaria, al fine di accelerare le procedure di ricerca e formazione di elementi aventi attitudine probatoria, quando ad oggetto vi siano dati informatici.

Si tratterebbe di una modalità di attuazione rapida di strumenti già esistenti, attivabile in caso di emergenza, ossia quando, ai sensi dell'art. 3, par. 2, lett. c) del Secondo protocollo, si realizzi una situazione in cui esiste un rischio significativo ed imminente per la vita o la sicurezza di qualsiasi persona fisica.

Orbene, la situazione di emergenza descritta all'art. 3 del Secondo protocollo e su cui si basano le procedure previste agli artt. 9 e 10 del Secondo protocollo⁸³⁹ si distingue dalla

⁸³⁶ Inoltre, la Parte richiesta che fornisce le informazioni o il materiale soggetti a condizione potrebbe chiedere alla Parte richiedente di spiegare, in relazione a tale condizione, l'uso fatto delle informazioni e del materiale.

⁸³⁷ Cfr., art. 9, par. 7, del Secondo protocollo.

⁸³⁸ In questi termini, CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 58 ss.

⁸³⁹ Invero, anche l'art. 12 del Secondo protocollo, nel disciplinare le squadre investigative comuni e le indagini congiunte, prevede che le informazioni ottenute con tali modalità possano essere usate per

situazione di urgenza prevista all'art. 25, par. 3, della Convenzione sulla criminalità informatica.

L'art. 25, par. 3 della Convenzione sulla criminalità informatica prevede che le richieste di assistenza reciproca siano fatte con mezzi di comunicazione accelerati in circostanze urgenti che, tuttavia, non raggiungano un determinato alto livello di emergenza, prevedendo un metodo più rapido per trasmettere o rispondere a una richiesta, a differenza dell'assistenza reciproca di emergenza che prevede una maggiore accelerazione ed obblighi più stringenti.

Invero, si dovrebbe ritenere che il ventaglio di ipotesi in cui sarebbe attivabile lo strumento di cui all'art. 25, par. 3 della Convenzione sulla criminalità informatica sia più ampio rispetto alle ipotesi previste dall'art. 10 del Secondo protocollo, in cui sono previsti presupposti assai stringenti.

L'art. 25, par. 3 della Convenzione sulla criminalità informatica consentirebbe una accelerazione minima delle procedure nei casi in cui si riscontrino rischi continui ma non imminenti per la vita o la sicurezza delle persone, la potenziale distruzione di prove determinata dal ritardo delle classiche procedure, la data ravvicinata di un processo o altri tipi di urgenza, mentre l'art. 10 del Secondo protocollo attiverebbe una procedura ad alta velocità in casi di particolare allarme⁸⁴⁰.

L'emergenza, quindi, imporrebbe una soglia più alta di rischio per l'attivazione di una procedura particolarmente accelerata. Il rischio deve qualificarsi come significativo e imminente⁸⁴¹. Sarebbero da escludere tutte le situazioni in cui il rischio per la vita o la sicurezza sia già passato o sia insignificante ovvero non sia imminente. Una soglia così elevata è necessaria perché alle richieste di emergenza è data la massima priorità rispetto a richieste che risultano essere urgenti o meno importanti, anche se sono state presentate in un momento precedente⁸⁴².

Si tratta, dunque, di un sistema a tre velocità. Volendo utilizzare una metafora, è come se gli strumenti viaggiassero su tre treni diversi: gli strumenti tradizionali per la ricerca di elementi aventi attitudine probatoria su un treno regionale, gli strumenti basati sull'urgenza su un Frecciabianca e gli strumenti attivabili in caso di emergenza su un Frecciarossa.

Tuttavia, i benefici relativi a rapidità ed efficienza delle indagini sono apprezzabili ed accettabili solo se in armonia con le esigenze di uniformità delle disposizioni applicabili e con la miglior tutela possibile dei diritti fondamentali⁸⁴³.

Dunque, in caso di emergenza, si applica un regime di doppio binario. Se tra gli Stati coinvolti non esiste un trattato o un accordo di assistenza reciproca sulla base di una legislazione uniforme, si attiva la disciplina di cui all'art. 10, par. 7 del Secondo protocollo, il quale richiede che ai principi ed alle regole dell'art. 10, si affianchino le

prevenire un'emergenza, nel caso in cui non siano stati stabiliti condizioni di rifiuto o di limitazioni d'uso con un accordo.

⁸⁴⁰ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 62 ss.

⁸⁴¹ Sono, ad esempio, i casi in cui vi siano persone in ostaggio e si teme per la loro vita o per la loro integrità fisica o altri danni comparabili, o casi in cui vi siano abusi sessuali su minori ovvero casi di attacchi terroristici e minacce per la sicurezza di infrastrutture critiche in cui esiste un rischio significativo e imminente per la vita o la sicurezza di una persona fisica, come attacchi a sistemi informatici di un ospedale.

⁸⁴² Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 36.

⁸⁴³ Così, V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 453.

regole previste per le richieste di mutua assistenza in assenza di accordi internazionali, di cui all'art. 27, parr. 2.b) e da 3 a 8, nonché all'art. 28, parr. da 2 a 4 della Convenzione sulla criminalità informatica.

Nello specifico, si tratta della comunicazione diretta tra autorità centrali; del vincolo alla *lex fori*, salvo casi di incompatibilità; della disciplina relativa ai motivi di rifiuto; della sospensione dell'esecuzione e dell'attivazione delle regole sul “dialogo” tra autorità; della clausola di riservatezza; della disciplina relativa alle condizioni.

Qualora, invece, esista già un trattato o un accordo, ai sensi dell'art. 10, par. 8 del Secondo protocollo, le regole di cui all'art. 10 del Secondo protocollo integreranno la disciplina del relativo trattato o accordo, a meno che gli Stati non decidano di comune accordo di adottare alcune o tutte le disposizioni della Convenzione, di cui al par. 7 dell'art. 10 del Secondo protocollo, in sostituzione delle regole dei trattati o accordi applicabili.

Oltre al contenuto standard della richiesta a norma del trattato o del diritto interno applicabile, la richiesta di assistenza reciproca di emergenza – che dovrà essere accettata anche in forma elettronica – dovrà indicare una descrizione dei fatti che dimostrano l'esistenza di una emergenza e spiegare il modo in cui l'assistenza richiesta è necessaria per rispondere all'emergenza.

La norma consente alla Parte richiesta di avviare un dialogo basato sulla istanza volta ad ottenere informazioni supplementari utili alla valutazione della richiesta di assistenza. Lo Stato richiedente dovrà fornire tali informazioni. Non sono previsti termini certi e ben definiti. Si richiede, tuttavia, che l'avvio del dialogo e l'invio delle informazioni avvenga in tempi rapidi. Pur nella nebulosità della formulazione, dovrebbe ritenersi che la rapidità debba essere garantita compiendo le attività necessarie nel minor tempo possibile, evitando attività inutili, superflue o sovrabbondanti che potrebbero inavvertitamente contribuire ad un risultato infausto⁸⁴⁴.

Lo Stato richiesto deve accertare la sussistenza di tutti i requisiti, tra cui lo stato di emergenza. Immediatamente dopo, deve rispondere rapidamente alla richiesta.

Siccome è fondamentale garantire la maggior rapidità possibile, l'art. 10, par. 5 del Secondo protocollo richiede agli Stati di indicare una persona della propria autorità centrale o di altre autorità ritenute responsabili di rispondere alle richieste di assistenza reciproca che sia disponibile ventiquattro ore su ventiquattro, sette giorni su sette.

In questo modo si consente di attivare rapidamente la procedura, perché è possibile procedere anche al di fuori del normale orario di lavoro contattando il personale competente ad esaminare le richieste di emergenza⁸⁴⁵.

Gli Stati possono determinare reciprocamente un canale alternativo per la trasmissione delle informazioni e dei dati elettronici ovvero di una copia anticipata di essi⁸⁴⁶. In tal modo, invece di utilizzare il classico canale di trasmissione degli elementi

⁸⁴⁴ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 63.

⁸⁴⁵ Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 63.

⁸⁴⁶ Inoltre, l'art. 10, par. 9 del Secondo protocollo consente a ciascuna Parte, al momento della firma o del deposito dello strumento di ratifica, accettazione o approvazione, di dichiarare che le richieste possono anche essere inviate direttamente alle sue autorità giudiziarie, o attraverso i canali dell'INTERPOL o al suo punto di contatto della Rete 24/7. In tutti questi casi, va inviata contemporaneamente una copia all'autorità centrale della Parte richiesta tramite l'autorità centrale della Parte richiedente. Se una richiesta è inviata direttamente all'autorità giudiziaria della Parte destinataria della richiesta e quest'ultima non è competente

aventi attitudine probatoria, essi possono decidere reciprocamente di utilizzare un canale diverso per accelerare ulteriormente la procedura o per garantire l'integrità dei dati o per altre ragioni⁸⁴⁷.

12. Le regole relative alla formazione della prova elettronica transfrontaliera vigenti negli Stati Uniti d'America

La difficoltà di ottenere un compendio avente attitudine probatoria di matrice digitale in circostanze che coinvolgono in qualche modo giurisdizioni o autorità straniere sono state a lungo al centro del dibattito dottrinale, giurisprudenziale e politico negli Stati Uniti d'America. Siccome i trattati di mutua assistenza per la ricerca e formazione delle prove digitali non risultano più adeguati, il legislatore statunitense ha ritenuto necessario prevedere nuovi meccanismi di cooperazione diretta tra gli *internet service provider* e gli Stati coinvolti nei processi penali, emanando il *Clarifying Lawful Overseas Use of Data Act*⁸⁴⁸, altrimenti conosciuto con l'acronimo *CLOUD Act*⁸⁴⁹.

a trattare la richiesta, essa invia la richiesta all'autorità nazionale competente e informa direttamente lo Stato richiedente di quanto compiuto.

⁸⁴⁷ Ad esempio, in caso di emergenza, le autorità possono decidere di trasmettere le prove direttamente ad una autorità investigativa o ad un'autorità giudiziaria dello Stato richiedente che utilizzerà i dati elettronici, invece di utilizzare i classici canali che prevedono lunghi passaggi "a catena" tra le autorità. Cfr., CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, cit., p. 63.

⁸⁴⁸ CONGRESS.GOV., *Text - H.R.4943 - 115th Congress (2017-2018): CLOUD Act.*, 6 febbraio 2018, disponibile al link: <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>. Il testo del *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) è incluso nel *Consolidated Appropriations Act* 2018, H.R. 1625, 23 March 2018, disponibile al link: [https://www.congress.gov/bill/115th-congress/house-bill/1625/related-](https://www.congress.gov/bill/115th-congress/house-bill/1625/related-bills?q=%7B%22search%22%3A%5B%22consolidated+appropriations+act%22%5D%7D&r=3)

[bills?q=%7B%22search%22%3A%5B%22consolidated+appropriations+act%22%5D%7D&r=3](https://www.congress.gov/bill/115th-congress/house-bill/1625/related-bills?q=%7B%22search%22%3A%5B%22consolidated+appropriations+act%22%5D%7D&r=3).

⁸⁴⁹ Per un approfondimento sul tema, H.H. ABRAHA, *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, in *International Journal of Law and Information Technology*, 29, 2021, p. 118 ss.; ID., *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, in *Information & Communication Technology Law*, 3, 2020, p. 324 ss.; ID., *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, in *International Data Privacy Law*, 3, 2019, p. 207 ss.; P. ALLISON, A. HINDOCHA, *US Global Cybercrime Cooperation: A Brief Explainer*, in *Third Way*, 26 giugno 2020, disponibile al link: <https://www.jstor.org/stable/resrep25041>; V. BALBUZANOVA, *Don't Kill the Messenger How the New Technologies Used by Internet-Based Communications Providers are Gutting Compelled Disclosure Laws*, in *Journal of Law & Cyber Warfare*, 1, 2020, p. 139; S. BILGIC, *Something Old, Something New, And Something Moot: The Privacy Crisis Under the CLOUD Act*, in *Harvard Journal of Law & Technology*, 1, 2018, p. 321 ss.; T. CHRISTAKIS, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, in AA.VV., *Cybersecurity and Privacy in a Globalized World – Building Common Approches* (P. MILCH, S. BENTHALL eds.), New York, 2019, p. 60 ss.; J. DASKAL, *Unpacking the CLOUD Act*, in *Eucrim*, 4, 2018, p. 220 ss.; ID., *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, in *Stanford Law Review Online*, 71, 2018, p. 9 ss.; J. DASKAL, P. SWIRE, *Why the CLOUD Act is Good for Privacy and Human Rights*, in www.justsecurity.org, 14 marzo 2018, p. 1 ss., disponibile al link: <https://www.justsecurity.org/53847/cloud-act-good-privacy-human-rights/>; J. GALBRAITH, *United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data*, in *American Journal of International Law*, 1, 2020, p. 124 ss.; ID., *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, in *The American Journal of International Law*, 3, 2018, p. 486 ss.; E.B. KIM, *U.S.-U.K. Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act*, in *Washington Journal of Law, Technology & Arts*, 3, 2020, p. 247 ss.; R.K. KNAKE, *Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online*

La nuova legge mira a facilitare l'accesso transfrontaliero delle autorità di contrasto ai dati, garantendo allo stesso tempo la tutela della vita privata e di altri diritti fondamentali. Inoltre, attualmente rappresenta il prototipo di un nuovo approccio alla cooperazione internazionale in materia penale⁸⁵⁰.

Approvato il 23 marzo 2018 dal Congresso degli Stati Uniti, il CLOUD Act aggiorna l'ormai risalente disciplina relativa alle richieste di ricezione dei dati posseduti dai *service provider*.

Invero, la nuova disciplina innova e modifica lo *Stored Communications Act (SCA)* del 1986⁸⁵¹, ritenuto da tempo obsoleto ed incompatibile con i recenti sviluppi tecnologici⁸⁵², chiarendo gli ambiti di applicazione geografica delle richieste provenienti dalle autorità giudiziarie degli Stati Uniti e fornendo ai *service provider* nuovi strumenti per contestare le richieste in conflitto con il sistema legislativo degli altri Stati. Inoltre, il CLOUD Act modifica diverse altre disposizioni dell'*Electronic Communications Privacy Act (ECPA)*⁸⁵³ per creare un quadro normativo che consenta ai fornitori di servizi statunitensi di divulgare i dati archiviati negli Stati Uniti a determinati Paesi stranieri in base a legittimi ordini provenienti dall'estero.

Obiettivo del CLOUD Act è consentire, tramite un *warrant* o un *subpoena*, alle forze dell'ordine federali di obbligare i *service provider* con sede negli Stati Uniti a fornire i dati richiesti archiviati sui *server*, indipendentemente dal fatto che i dati siano archiviati negli Stati Uniti o in un territorio straniero. Il legislatore statunitense ha previsto un nuovo approccio efficiente, a tutela della privacy e dei diritti fondamentali, garantendo al tempo

Freedom and Cybersecurity, cit., p. 7 ss.; N. KUSHWAHA, P. ROGUSKI, B.W. WATSON, *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*, in AA.VV., *2020 12th International Conference on the Cyber Conflict (CyCon)* (T. JANČÁRKOVÁ, L. LINDSTRÖM, M. SIGNORETTI, I. TOLGA, G. VISKY eds.), Tallin, 2020, p. 43 ss.; L. LUPÁRIA DONATI, *Privacy, diritti della persona e processo penale*, in *Riv. Dir. proc.*, 6, 2019, p. 1448; S. PARSHEERA, P. JHA, *The Move Toward Direct Data Access Agreements*, in *Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?*, Carnegie Endowment for International Peace, 2020, p. 15 ss.; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, in *Computer Law & Security Review*, 38, 2020, p. 1 ss., disponibile al link: <https://www.sciencedirect.com/science/article/pii/S0267364920300479>; J. SHURSON, *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, in *International Journal of Law and Information Technology*, 28, 2020, p. 167 ss.; A.K. WOODS, P. SWIRE, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, in *Lawfare*, 6 febbraio 2018, disponibile al link: <https://www.lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems>.

⁸⁵⁰ Sul punto, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 324 ss.

⁸⁵¹ L'SCA costituisce il Titolo II dell'*Electronic Communications Privacy Act*. Sullo *Stored Communications Act*, per un approfondimento, O.S. KERR, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, in *George Washington Law Review*, 72, 2004, p. 1208 ss.

⁸⁵² Uno studio ha evidenziato che a causa delle disposizioni di blocco della SCA, un gran numero di richieste di mutua assistenza giudiziaria per i dati sui contenuti doveva passare attraverso il Dipartimento di Giustizia degli Stati Uniti e il sistema giudiziario federale. Ciò comportava ritardi tali da rendere impraticabile la ricerca e formazione delle prove elettroniche, con richieste di *routine* che richiedevano da otto a tredici mesi per essere soddisfatte. Sul punto, G. KENT, *Sharing Investigation-Specific Data with Law Enforcement – An International Approach*, in *Stanford Public Law Working Paper*, 2014, disponibile al link: <http://www.ssrn.com/abstract=2472413>; J. SHURSON, *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, cit., p. 168.

⁸⁵³ *Electronic Communications Privacy Act* of 1986, Pub. L. 99-508, 100 Stat. 1848, 1860 (1986).

stesso un accesso effettivo ai dati elettronici collocati in un Paese straniero, a tutela della sicurezza pubblica e dello Stato di diritto⁸⁵⁴.

Il CLOUD Act ha tratto origine dal noto caso *Microsoft Corp. vs. United States*⁸⁵⁵. La vicenda giudiziaria cominciò nel 2013 e si concluse solo nel 2018, con l'entrata in vigore del nuovo testo legislativo, che pose fine alla questione, poiché si modificò lo *Stored Communications Act (SCA)*⁸⁵⁶, la legge al centro della contesa.

⁸⁵⁴ In tal senso, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 324.

⁸⁵⁵ *United States v. Microsoft Corp.*, No 17-2 (US, 11 January 2018). Per un approfondimento sul caso *Microsoft Corp. v. United States*, S. CARRERA, G.G. FUSTER, E. GUILD, V. MITSILEGAS, *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, in *Centre for European Policy Studies*, 8 luglio 2015, disponibile al link: <https://www.ceps.eu/ceps-publications/access-electronic-data-third-country-law-enforcement-authorities-challenges-eu-rule-law/>; R.J. CURRIE, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, in *Canadian Yearbook of International Law*, 54, 2017, p. 63 ss.; J. DASKAL, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, cit., *passim*; P. DE HERT, J. THUMFART, *The Microsoft Ireland Case, the Cloud Act and the Cyberspace Sovereignty Trilemma*, in *Jusletter IT*, 12, 2021, p. 373 ss.; J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 487 ss.; D.J.B. SVANTESSON, Q.C.F. GERRY, *Access to Extraterritorial Evidence: The Microsoft Cloud Case and beyond*, in *Computer Law and Security Review*, 4, 2015, p. 478 ss.

⁸⁵⁶ In poche battute, siccome il procedimento di mutua assistenza giudiziaria sarebbe risultato lento e avrebbe potuto ostacolare le indagini, il *Federal Bureau of Investigation* (FBI) preferì applicare lo *Stored Communications Act (SCA)* e chiese a Microsoft le informazioni presenti nei propri server situati in Irlanda, sul presupposto che la società di Redmond avesse il pieno controllo sui dati, avendo accesso ad essi anche dall'interno degli Stati Uniti. A detta degli FBI, il luogo in cui i dati sono stati memorizzati doveva essere ritenuto irrilevante. Microsoft si oppose, in quanto riteneva che l'SCA non potesse essere applicato ai dati ubicati al di fuori del territorio degli Stati Uniti.

Più nello specifico, il 4 dicembre 2013, nell'ambito di un'indagine relativa al traffico di droga, un magistrato statunitense emise un mandato che autorizzava la perquisizione e il sequestro di dati associati a un *account* di posta elettronica. I dati erano archiviati presso dei locali di proprietà mantenuti, controllati o gestiti da *Microsoft Corporation*. La società era solita archiviare la maggior parte dei dati di comunicazione e dei dati di contenuto sui server vicini alla posizione geografica dichiarata dall'utente durante la configurazione dell'*account* di posta elettronica, senza verificare la posizione geografica degli utenti. Microsoft consegnò i metadati e i dati relativi all'*account* che aveva archiviato negli Stati Uniti, ma si oppose alla consegna dei dati di contenuto e di altro tipo perché conservati sui server allocati in Irlanda. Secondo la società, il mandato basato sulla SCA non poteva richiedere dati archiviati all'estero, poiché la SCA non prevedeva la possibilità per i mandati di richiedere dati conservati oltre i confini nazionali.

In primo grado, il giudice respinse le argomentazioni di Microsoft e rilevò che il mandato contemplato dalla SCA aveva il valore di un "atto misto" tra un convenzionale "*search warrant*" ed un "*subpoena*", che richiede la produzione di dati indipendentemente dalla loro ubicazione purché i dati siano in possesso, custodia o controllo di Microsoft.

Microsoft impugnò la sentenza e la Court of Appeal for the Second Circuit di New York la annullò sul presupposto che il mandato avesse efficacia solo entro i confini degli Stati Uniti. Secondo la Corte d'Appello, non si può essere certi degli obblighi e delle leggi estere (in particolare, dell'Irlanda e dell'Unione europea) imposte ai fornitori di servizi in internet che memorizzano dati digitali. Inoltre, la Corte d'Appello basò la propria decisione sul principio già previsto con la sentenza *Morrison c. National Australia Bank*, secondo cui le leggi del Congresso debbano sempre essere ritenute applicabili solo all'interno della giurisdizione degli Stati Uniti, se non diversamente disposto. Il caso è arrivato sino alla Corte Suprema degli Stati Uniti, davanti alla quale è stata istruita e discussa. Tuttavia, prima che la Corte potesse emettere una decisione, il Congresso approvò il CLOUD Act. Di conseguenza, la Corte Suprema ha archiviato il processo il 17 aprile 2018, dopo essere stata informata dalle parti dell'adozione del CLOUD Act, consentendo così l'emissione di un nuovo mandato per ottenere le informazioni necessarie da Microsoft.

Il CLOUD Act, dunque, ha risolto la questione, prevedendo che l'ordine va eseguito ogni volta in cui il fornitore di servizi abbia il possesso, la custodia o il controllo dei dati, indipendentemente dal luogo in

Il CLOUD Act apporta tre chiarimenti significativi. Innanzitutto, per quanto attiene alla giurisdizione, autorizza esplicitamente le forze dell'ordine a obbligare un fornitore di servizi a produrre i dati degli utenti indipendentemente dal luogo in cui si trovano il fornitore e i dati ricercati, secondo il principio della “non territorialità dei dati”⁸⁵⁷. Infatti, il CLOUD Act consente al *search warrant* emesso ai sensi della SCA di spiegare i propri effetti anche oltre i confini degli Stati Uniti. *In secundis*, individua un preciso criterio di giurisdizione, rendendo irrilevante il luogo di ubicazione dei dati, a favore di quello in cui è stanziato il fornitore di servizi e, in una certa misura, di residenza e nazionalità dell'utente. Infine, il CLOUD Act introduce un nuovo quadro per affrontare il potenziale rischio di conflitto con le leggi straniere⁸⁵⁸.

Il testo è divisibile in due parti: le disposizioni per l'accesso degli Stati Uniti ai dati archiviati all'estero e le disposizioni per creare accordi esecutivi per l'accesso dall'estero ai dati archiviati negli Stati Uniti.

Nello specifico, per quanto attiene all'accesso delle forze dell'ordine degli Stati Uniti ai dati archiviati all'estero, la modifica apportata all'SCA consente di imporre ai fornitori di servizi di divulgare i dati dei propri clienti alle autorità statunitensi indipendentemente dal luogo in cui sono ubicati tali dati, purché l'*internet service provider* sia una società soggetta alla giurisdizione degli Stati Uniti – anche se straniera⁸⁵⁹ – ed abbia il possesso, la custodia o il controllo dei dati, anche se archiviati in un altro Stato⁸⁶⁰.

cui sia conservate le comunicazioni, registrazioni o altre informazioni. Sul punto, J. SHURSON, *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, cit., p. 170 ss. V., inoltre, H.H. ABRAHA, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, cit., p. 208; V. BALBUZANOVA, *Don't Kill the Messenger How the New Technologies Used by Internet-Based Communications Providers are Gutting Compelled Disclosure Laws*, cit., p. 139; J. DASKAL, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, cit., p. 9 ss.; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 4 ss.; G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, cit., p. 109 ss.; O. SALLAVACI, *Rethinking Criminal Justice in Cyberspace: The EU E-Evidence Framework ad a New Model of Cross-Border Cooperation in Criminal Matters*, in AA.VV., *Policing in the Era of AI and Smart Societies* (H. JAHANKHANI, B. AKHGAR, P. COCHRANE, M. DASTBAZ eds.), Cham, 2020, p. 19.

⁸⁵⁷ Sul principio della non territorialità dei dati, J. DASKAL, *The Un-Territoriality of Data*, in *The Yale Law Journal*, 2, 2015, p. 326 ss.; O.S. KERR, *The Next Generation Communications Privacy Act*, in *University of Pennsylvania Law Review*, 2, 2014, p. 373 ss. In argomento, v. anche, UNODC, *Comprehensive Study on Cybercrime*, New York, 2013, p. 183 ss.

⁸⁵⁸ In tal senso, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 330.

⁸⁵⁹ Nello specifico, il CLOUD Act sembrerebbe applicabile anche ai *provider* di posta elettronica, alle società di telecomunicazioni, ai siti di social media ed ai fornitori di servizi di *cloud*, indipendentemente dal fatto che siano stabiliti negli Stati Uniti o in un altro Stato. In pratica, ogni società straniera con un ufficio, una sede o una filiale negli Stati Uniti sarebbe soggetta al CLOUD Act.

⁸⁶⁰ Così, H.H. ABRAHA, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, cit., p. 208; J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 489; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 4. Per uno studio che tenta di dare delle soluzioni interpretative al concetto di “società soggetta alla giurisdizione degli Stati Uniti” e di “possesso, custodia o controllo”, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 333 ss.; W. MAXWELL, M.W. BRENNAN, A.A. SURA, *Demystifying the US CLOUD Act: Assessing the Law's Compatibility with International Norms and the GDPR*, Washington, 2019, p. 4 ss., disponibile al link: https://www.hoganlovells.com/-/media/hoganlovells/pdf/2019/2019_01_15_whitepaper_demystifying_the_us_cloud_act.pdf; W. RIDGWAY, *Understanding The CLOUD Act's Expansive Reach*, in *Mondaq*, 13 dicembre 2018, disponibile al link: <https://www.mondaq.com/unitedstates/privacy-protection/763706/understanding-the-cloud-act39s-expansive-reach>.

Per emettere un *warrant*, una Corte degli Stati Uniti deve essere convinta che vi siano indizi tali da far ritenere che si sia verificato un crimine e che le prove da ottenere tramite *warrant* siano direttamente correlate a tale crimine.

Anche se la legge individua requisiti rigorosi⁸⁶¹, il legislatore statunitense ha ritenuto opportuno costituire in capo ai fornitori di servizi il diritto di contestare le richieste delle forze dell'ordine, quando ritiene sussistenti i seguenti tre requisiti: si ritiene che i dati ricercati siano relativi a una persona che non abbia la cittadinanza statunitense o che non risieda negli Stati Uniti; la divulgazione dei dati creerebbe un rischio materiale di violazione della legge straniera; il Paese straniero la cui legge potrebbe essere violata ha stipulato un accordo esecutivo ai sensi del CLOUD Act⁸⁶². Il tribunale decide secondo una “*comity analysis*”, valutando otto fattori, tra cui gli interessi degli Stati Uniti e gli interessi dello Stato straniero “qualificato” al blocco della divulgazione dei dati⁸⁶³.

Il fornitore di servizi può adire il tribunale per ottenere l'annullamento o la modificazione dell'ordine entro 14 giorni dalla notifica⁸⁶⁴. Tuttavia, questo termine stringente potrebbe non essere sufficiente ad attivare tale garanzia a causa delle difficoltà della società nel determinare l'ubicazione del *server* e compiere una ponderata valutazione relativa alla legittimità della richiesta dell'autorità statunitense. Pertanto, la dottrina ha ritenuto che il rigoroso limite di tempo, unito alla minaccia di sanzioni, possa incentivare i fornitori di servizi a rivelare in ogni caso i dati, senza compiere un'attenta valutazione dei requisiti richiesti dal CLOUD Act⁸⁶⁵.

Vi è poi chi si è chiesto se uno Stato straniero “qualificato” secondo i criteri del CLOUD Act possa opporsi ad un ordine di divulgazione emesso ai sensi del CLOUD Act. Vi è chi ritiene che, nel prevedere criteri basati sulla nazionalità e sulla posizione dell'utente, il CLOUD Act consentirebbe agli Stati stranieri “qualificati” di opporsi a un *warrant* emesso secondo le regole dell'SCA⁸⁶⁶. Sul punto, va sottolineato che il CLOUD Act consente ai fornitori di servizi di informare lo Stato straniero “qualificato” mediante notifica dell'avvio del procedimento relativo alla divulgazione di dati di un cittadino dello Stato informato o ivi residente da parte dell'autorità giudiziaria degli Stati Uniti⁸⁶⁷, allo scopo di consentire allo Stato straniero di intraprendere le proprie azioni legali, tra cui

⁸⁶¹ Così, J. DASKAL, *Privacy and Security Across Borders*, in *The Yale Law Journal Forum*, 128, 2019, p. 1029 ss.

⁸⁶² CLOUD Act, s 103(b) (codified at 18 USC. s 2703(h)). Per un'analisi dettagliata di ciascuno di questi requisiti, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 336 ss. Sui requisiti, v. anche, J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 489; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 4 ss.

⁸⁶³ In tal senso, J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 489.

⁸⁶⁴ CLOUD Act, s 103(b) (codified at 18 USC. s 2703(h)(2)(ii)).

⁸⁶⁵ Sul punto, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 339.

⁸⁶⁶ P.M. SCHWARTZ, *Legal Access to the Global Cloud*, in *Columbia Law Review*, 6, 2018, p. 1755, secondo il quale «*the ability of a foreign country to object to the extraterritorial use of an SCA warrant is present only when the cloud provider can reasonably point to the nationality and location of the user*».

⁸⁶⁷ CLOUD Act, s 103(b) (codified at 18 USC. s 2703(h)), ai sensi del quale «*It shall not constitute a violation of a protective order [...] for a provider [...] to disclose to the entity within a qualifying foreign government designated in an executive agreement [...], the fact of the existence of legal process [...] seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government*».

l'opposizione al procedimento⁸⁶⁸. I motivi specifici in base ai quali lo Stato straniero "qualificato" può opporsi al *warrant* emesso dalle autorità statunitensi dovrebbero essere oggetto di futuri negoziati, nell'ambito degli accordi esecutivi⁸⁶⁹.

Tuttavia, non sembrano esistere elementi – né a carattere normativo, né in dottrina – che facciano ritenere possibile l'attivazione di un meccanismo diretto di tutela da parte delle persone coinvolte. Invero, i singoli individui non possono impugnare un *warrant* ai sensi del CLOUD Act, di talché la tutela dei loro diritti dipende dalle impugnazioni che eventualmente vorranno proporre i legittimati.

Ma la novità più rilevante del CLOUD Act risiede nella sua seconda parte, relativa alle regole sull'accesso del governo straniero ai dati detenuti dai fornitori di servizi statunitensi⁸⁷⁰.

In questa seconda parte, il CLOUD Act affronta l'opposta questione relativa alle attività degli altri Stati nei casi in cui è necessario accedere ai contenuti delle comunicazioni detenute dai fornitori di servizio statunitensi.

Invero, le autorità di contrasto sono tenute a presentare una richiesta basata sul principio di mutua assistenza al governo statunitense, anche se sono alla ricerca di dati relativi a un proprio cittadino. Si tratta di un processo dispendioso in termini di tempo⁸⁷¹, che prevede un esame della richiesta da parte del Dipartimento di Giustizia, un ricorso in tribunale da parte di un ufficio del procuratore statunitense per ottenere un mandato per conto del governo straniero e una successiva revisione da parte del Dipartimento di Giustizia prima che i dati vengano infine divulgati⁸⁷².

⁸⁶⁸ Così, anche, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 339.

⁸⁶⁹ Il *Department of Justice USA* ha recentemente ribadito che i governi stranieri sono liberi nei negoziati di individuare restrizioni che impediscano agli Stati Uniti di utilizzare i *warrant* oggetto di accordo per richiedere i dati dei propri cittadini o delle persone residenti sul proprio territorio. Sul punto, si veda, US DEPARTMENT OF JUSTICE, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, aprile 2019, p. 12, disponibile al link: <https://www.justice.gov/dag/page/file/1153436/download>.

⁸⁷⁰ CLOUD Act, s 105(a) (codified at 18 USC. s 2523).

⁸⁷¹ In un'audizione davanti al Committee on the Judiciary - U.S. House of Representatives, intitolata *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era*, R.W. Downing, Acting Deputy Assistant Attorney General, ha dichiarato che l'attuale sistema basato sui trattati di mutua assistenza giudiziaria non è concepito «to handle the growing demands for digital evidence. Already, the Department faces significant challenges in responding to the enormous volume of foreign demands with the requisite speed». Il testo dell'intervento è reperibile al link: <https://docs.house.gov/meetings/JU/JU00/20170615/106117/HHRG-115-JU00-Wstate-DowningR-20170615.pdf>.

Uno studio del 2013 ha evidenziato che il governo degli Stati Uniti impiega in media dieci mesi per rispondere ad una richiesta di mutua assistenza, anche nelle situazioni in cui è più semplice decidere sull'invio dei dati. Sul punto, R.A. CLARKE, M. MORELL, G. STONE, C. SUSTEIN, P. SWIRE, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 18 dicembre 2013, disponibile al link: https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report; J. DASKAL, *Unpacking the CLOUD Act*, cit., p. 222.

⁸⁷² Per la descrizione del procedimento, G. KENT, *The Mutual Legal Assistance Problem Explained*, in CIS Blog – The Center for Internet and Society, 23 febbraio 2015, disponibile al link: <http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained>. V., inoltre, P.J. PULLEN, *Nail in the MLAT Coffin: Examining Alternative Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing*, in *North Carolina Journal of International Law*, 4, 2019, p. 1 ss. Per ulteriori studi sul funzionamento delle procedure di mutua assistenza e sulla necessità di un intervento riformistico, P. SWIRE, J.D. HEMMINGS, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, in *N.Y.U. Annual Survey of*

La nuova disciplina introdotta con il CLOUD Act consente alle forze dell'ordine degli Stati "qualificati" di accedere ai contenuti delle comunicazioni detenute negli Stati Uniti, senza attivare un procedimento basato sulle regole dei trattati di mutua assistenza giudiziaria in materia penale e rivolgendosi direttamente agli *internet service provider* con sede negli Stati Uniti.

Per realizzare ciò, al fine di velocizzare le attività connesse alla ricerca e formazione delle prove elettroniche transnazionali, il CLOUD Act ha previsto la necessaria redazione e conclusione di accordi bilaterali con gli Stati stranieri, i cc.dd. *executive agreements*, a seguito dei quali i Paesi terzi acquisiscono lo *status* di "*qualifying foreign government*"⁸⁷³.

Pertanto, per realizzare lo scopo di facilitare la cooperazione giudiziaria internazionale nella raccolta e nella trasmissione delle prove elettroniche⁸⁷⁴, l'esecutivo è autorizzato a stipulare accordi con gli Stati terzi, per consentire a questi ultimi di richiedere il contenuto delle comunicazioni elettroniche direttamente ai fornitori di servizi con sede negli Stati Uniti.

Con la conclusione dell'*executive agreement*, lo Stato estero otterrebbe un duplice vantaggio: potrà acquisire i contenuti delle comunicazioni conservate dai fornitori di servizi statunitensi attivando una procedura semplificata e potrà fornire una maggior tutela della privacy⁸⁷⁵ per i suoi cittadini o per le persone residenti sul proprio territorio quando le forze dell'ordine statunitensi cercano i loro dati⁸⁷⁶.

Non meno importante, come nota la dottrina, è la maggior garanzia offerta nei confronti dei diritti fondamentali ed assicurata dal sistema. Infatti, a differenza delle prassi di dubbia conformità con il rispetto dei diritti fondamentali, basate su misure a carattere unilaterale per accedere a dati, elusive delle norme poste a garanzia dei cittadini, il CLOUD Act assicurerebbe l'esistenza di meccanismi di apprensione dei dati informatici tali da eliminare la violazione del robusto corpo di diritti, sia sostanziali che procedurali, rappresentativi di condizioni necessarie per l'efficacia degli accordi bilaterali⁸⁷⁷.

Il CLOUD Act basa l'*executive agreement* essenzialmente su quattro fasi: 1) l'ammissibilità; 2) la negoziazione, la certificazione e l'acquisto dello *status* di

American Law, 4, 2016, p. 687 ss.; P. SWIRE, J. HEMMINGS, S. VERGNOLLE, *A Mutual Legal Assistance Case Study: The United States and Francia*, in *Wisconsin International Law Journal*, 2, 2017, p. 323 ss.

⁸⁷³ Il CLOUD Act definisce il "*qualifying foreign government*" come «*a foreign government with which the United States has an executive agreement [-]; and the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5)*». Cfr., CLOUD Act, s 103 (b) (codified at 18 USC. s 2703(h)(1)(A)(i)-(ii)).

⁸⁷⁴ In questo senso, M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 5 ss.

⁸⁷⁵ Accanto a chi ritiene che la nuova disciplina migliori la tutela della privacy e delle libertà rispetto a un mondo senza una legislazione dedicata, tra cui J. DASKAL, P. SWIRE, *Why the CLOUD Act is Good for Privacy and Human Rights*, cit., p. 1 ss., vi è chi ritiene che le modifiche apportate dal CLOUD Act alla disciplina relativa all'accesso transfrontaliero ai dati abbia generato un *vulnus* al diritto alla privacy e, più in generale, ai diritti umani. Sul punto, J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 492.

⁸⁷⁶ Così, B. BARNETT, J.A. BROWN, O. FASSHAUER, V.L. FRANCIS, T.E. YALE, *Forecasting the Impact of the New US CLOUD Act*, Filadelfia, 2018, p. 3 ss., disponibile al link: <http://bit.ly/2ZEGBYB>; H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 341.

⁸⁷⁷ Sul punto, O. POLLICINO, M. BASSINI, *La proposta di Regolamento E-Evidence: osservazioni a caldo e possibili sviluppi*, in *medialaws.ue*, 26 ottobre 2018, p. 1 ss.

“*qualifying foreign government*”; 3) l’attuazione; 4) la revisione dell’*executive agreement*⁸⁷⁸.

Più specificamente, lo Stato terzo, per risultare idoneo alla negoziazione dell’accordo, deve disporre di una legge nazionale che offra una solida protezione della privacy e delle libertà rilevanti per la raccolta dei dati elettronici e per i rapporti con le autorità straniere⁸⁷⁹. Dunque, deve avere un adeguato quadro normativo in materia di criminalità informatica e prove elettroniche; deve rispettare i principi dello Stato di diritto e di non discriminazione; deve uniformarsi agli obblighi internazionali in materia di diritti fondamentali; deve agire con responsabilità e trasparenza per quanto attiene alla raccolta e all’uso dei dati elettronici⁸⁸⁰. Lo Stato deve non solo possedere in astratto tali requisiti sostanziali e procedurali, ma anche dimostrare in concreto di attuarli al proprio interno, poiché è solo così che può ottenere una fiducia minima, tale da abbattere le preoccupazioni relative a questioni inerenti agli interessi politici e alla protezione dei diritti umani⁸⁸¹.

L’*Attorney General*, con il consenso del Segretario di Stato, può negoziare un *executive agreement* solo con uno Stato estero che soddisfi tali criteri di ammissibilità. Raggiunto l’accordo, l’*Attorney General* presenta una certificazione scritta al Congresso⁸⁸² dove attesta il possesso dei requisiti in capo allo Stato terzo e conferisce lo *status* di “*qualifying foreign government*”⁸⁸³.

Una volta reso esecutivo l’accordo⁸⁸⁴, il procedimento per la ricerca e formazione della prova elettronica transnazionale seguirà le regole dello Stato richiedente.

Non è richiesto il requisito della doppia incriminabilità⁸⁸⁵. Uno Stato può emettere un ordine rivolto agli *internet service provider* statunitensi solo se si tratta di un procedimento che abbia ad oggetto un reato grave⁸⁸⁶. Nulla è stabilito in merito a quali possano essere i reati gravi. È certo che tra i reati gravi sono annoverati quelli di matrice

⁸⁷⁸ Per una descrizione approfondita di ogni singola fase, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 341 ss. V., inoltre, J. GALBRAITH, *United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data*, cit., p. 125 ss.

⁸⁷⁹ *CLOUD Act*, s 105(a) (codified at 18 USC. s 2523(b)(1)). Sul punto, H.H. ABRAHA, *How compatible is the US ‘CLOUD Act’ with cloud computing? A brief analysis*, cit., p. 209 ss.; J. DASKAL, *Unpacking the CLOUD Act*, cit., p. 222.

⁸⁸⁰ *CLOUD Act*, s 105(a) (codified at 18 USC. s 2523(b)(1)(B)(i)).

⁸⁸¹ In tal senso, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 342 ss.

⁸⁸² Il Congresso ha limitati poteri di intervento, potendo soltanto emettere una risoluzione di disapprovazione. Il vero potere decisionale è affidato all’organo esecutivo, il quale ha il compito di verificare e certificare i governi stranieri, senza che sia previsto alcun controllo giudiziario o amministrativo. Cfr., *CLOUD Act*, s 105(a) (codified at 18 USC. s 2523(c)).

⁸⁸³ Cfr., *CLOUD Act*, s 105 (a) (codified at 18 USC. s 2523(b)). Così, J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 490 ss.; R.K. KNAKE, *Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity*, cit., p. 8.

⁸⁸⁴ L’Accordo è soggetto a revisione periodica, da effettuare ogni cinque anni, da parte del governo degli Stati Uniti per determinare se il *qualifying foreign government* soddisfi i requisiti del *CLOUD Act*. Cfr., *CLOUD Act*, s 105(a) (codified at 18 USC. s 2523(e)(1)–(2)).

⁸⁸⁵ Critico sul punto, H.H. ABRAHA, *How compatible is the US ‘CLOUD Act’ with cloud computing? A brief analysis*, cit., p. 211.

⁸⁸⁶ Cfr., *CLOUD Act*, s 105 (a) (codified at 18 USC. s 2523(b)(4)(D)(i)).

terroristica⁸⁸⁷. Tuttavia, non si stabilisce se l'*executive agreement* debba preferire l'individuazione di essi mediante un criterio quantitativo, qualitativo o misto.

Per quanto riguarda l'oggetto dell'ordine, il CLOUD Act richiede che ogni ordine emesso da uno Stato debba identificare una persona, un account, un indirizzo o un dispositivo personale specifico, o qualsiasi altro identificatore specifico⁸⁸⁸.

Ogni ordine deve essere conforme alle leggi nazionali dello Stato di emissione e deve essere «*based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation*»⁸⁸⁹. Inoltre, ogni ordine deve essere soggetto a revisione o controllo da parte di un tribunale, giudice, magistrato o altra autorità indipendente dello Stato di emissione⁸⁹⁰.

Una volta ottenuti i dati dai fornitori di servizi con sede negli Stati Uniti, lo Stato deve rispettare requisiti minimi di sicurezza, utilizzo, gestione e diffusione. La legge indica solo alcune attività necessarie, i cui dettagli sono lasciati alla libera definizione dello Stato. Invero, il CLOUD Act non prescrive alcuno standard di sicurezza, ma richiede solamente che l'altro Stato archivi i dati in un sistema sicuro⁸⁹¹.

Merita attenzione l'ambito di operatività particolarmente stringente dell'*executive agreement*. Il CLOUD Act individua una serie di «*target limitation*» – delle limitazioni dei bersagli – che di fatto restringono la portata della nuova disciplina. Invero, lo Stato terzo può richiedere solo i dati di cittadini non statunitensi stanziati su territori diversi da quello degli Stati Uniti, mentre è vietato richiedere – direttamente o indirettamente – dati di cittadini e persone residenti negli Stati Uniti⁸⁹². È, inoltre, vietata l'accesso a contenuti di comunicazione di cittadini statunitensi residenti all'estero. In altre parole, lo Stato qualificato non può nemmeno richiedere i dati dei suoi cittadini o residenti se questi saranno, in ultima battuta, utilizzati contro uno statunitense⁸⁹³.

Sembra lecito riflettere su quale sia l'effettivo spazio di operatività di una disciplina così limitante nei confronti degli Stati terzi – e, di conseguenza, anche degli Stati membri dell'Unione europea – i quali, probabilmente, applicheranno le regole previste nel futuro *executive agreement* per un numero limitato di casi. Ciò, alla luce anche della previsione che vuole che gli Stati adottino procedure volte a ridurre al minimo le ipotesi di

⁸⁸⁷ Per un rilievo critico relativo all'assenza di una precisa definizione di «reato grave» ai sensi del CLOUD Act, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 346 ss.

⁸⁸⁸ Cfr., CLOUD Act, s. 2523(b)(4)(D)(ii)). Vedi, inoltre, O.S. KERR, *The Next Generation Communications Privacy Act*, cit., p. 375 ss.; J. DASKAL, *Privacy and Security Across Borders*, cit., p. 1029.

⁸⁸⁹ Cfr., CLOUD Act, s. 105 (a) (codified at 18 USC. s. 2523(b)(4)(D)(iv)). Lo standard richiesto è evidentemente più basso rispetto a quello previsto nei trattati di mutua assistenza, i quali richiedono la «*probable cause*». Sul punto, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 347.

⁸⁹⁰ Cfr., CLOUD Act, s. 105(a) (codified at 18 USC. s. 2523(b)(4)(D)(v)). Il riferimento ad altre autorità indipendenti lascerebbe pensare che anche autorità diverse da quelle appartenenti alla magistratura possano approvare gli ordini. Ciò ha attirato le critiche della dottrina. Per tali rilievi, G. NOJEM, *Cloud Act Implementation Issue*, in *Lawfareblog*, 10 luglio 2018, disponibile al link: <http://bit.ly/2FkTU8Y>.

⁸⁹¹ Così, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 350. Cfr., CLOUD Act, s. 105(a) (codified at 18 USC. s. 2523(b)(4)(F)–(H)).

⁸⁹² Cfr., CLOUD Act, s. 105(a) (codified at 18 USC. s. 2523(b) (4) (A)–(B)). V. anche, CLOUD Act, s. 103 (b) (codified at 18 USC. s. 2703(h)(5)). Per ottenere l'accesso al contenuto delle comunicazioni di una persona statunitense, lo Stato terzo dovrà attivare le classiche procedure previste nei trattati di mutua assistenza giudiziaria. Sul punto, J. DASKAL, *Unpacking the CLOUD Act*, cit., p. 220.

⁸⁹³ In tal senso, H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, cit., p. 345 ss.

acquisizione, conservazione e diffusione delle informazioni relative a cittadini statunitensi, ingabbiando di fatto una seria ed efficiente lotta alla criminalità operante nel fluido terreno del *web*.

Bisognerebbe chiedersi se tali previsioni non finiranno per rendere inutili i nuovi strumenti di cooperazione, perché gli Stati tenteranno di utilizzare espedienti volti ad eludere la nuova disciplina, mediante *spy-software* avanzati che rimetteranno in discussione i principi alla base della nuova cooperazione giudiziaria per la formazione delle prove elettroniche.

Infine, non si può non evidenziare come il CLOUD Act sembri concedere ai fornitori di servizi un enorme potere di mediazione tra i loro interessi commerciali, i diritti umani e gli interessi pubblicistici relativi alla tutela della sicurezza e alla lotta alla criminalità.

Il primo *executive agreement* è stato firmato il 3 ottobre 2019 tra gli Stati Uniti e il Regno Unito⁸⁹⁴. L'accordo bilaterale si candida ad essere un modello su cui basare i futuri accordi tra Stati Uniti e altri Paesi⁸⁹⁵.

Per facilitare l'accordo⁸⁹⁶, il Parlamento britannico ha approvato il *Crime (Overseas Production Orders) Act 2019*⁸⁹⁷, che crea un nuovo ordine di produzione all'estero da utilizzare per obbligare i fornitori di servizi aventi sede in un altro Stato a produrre i dati elettronici⁸⁹⁸.

⁸⁹⁴ Cfr., *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, U.S.-UK Data Access Agreement [CS USA No.6/2019]. L'accordo bilaterale è stato firmato a Washington da William Barr, *U.S. Attorney General*, e da Priti Patel, *UK Home Secretary*. Il testo è consultabile al link: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. Per un approfondimento sull'accordo, J. GALBRAITH, *United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data*, cit., p. 124 ss.; N. KUSHWAHA, P. ROGUSKI, B.W. WATSON, *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*, cit., p. 51 ss.; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 8 ss. V., inoltre, R.K. KNAKE, *Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity*, cit., p. 8.

⁸⁹⁵ In tal senso, J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, cit., p. 492; ID., *United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data*, cit., p. 126.

⁸⁹⁶ Si veda, in questo senso, P. SWIRE, J.D. HEMMINGS, *Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act*, in *Lawfare*, 13 settembre 2018, disponibile al link: <https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act>.

⁸⁹⁷ *Crime (Overseas Production Orders) Act 2019* (c. 5), disponibile al link: <https://www.legislation.gov.uk/ukpga/2019/5/contents/enacted>. V., inoltre, H.H. ABRAHA, *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, cit., p. 136; J. SHURSON, *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, cit., p. 181.

⁸⁹⁸ Anche l'Australia, in vista di un accordo bilaterale basato sul CLOUD Act, ha recentemente introdotto l'*International Production Orders Bill 2020*. Per un'analisi dettagliata del *bill*, P. SWIRE, *Comments on Australian Legislation to Enable the Negotiation of a U.S. CLOUD Act Executive Agreement*, in *Cross-Border Data Forum*, 11 maggio 2020, disponibile al link: <https://www.crossborderdataforum.org/comments-on-australian-legislation-to-enable-the-negotiation-of-a-u-s-cloud-act-executive-agreement/>. V., inoltre, A. BARBASCHOW, *New Bill to Prepare Australian Law Enforcement for the US CLOUD Act*, in *ZDNet.com*, 5 marzo 2020, disponibile al link: <https://www.zdnet.com/article/new-bill-to-prepare-australian-law-enforcement-for-the-us-cloud-act/>. Il testo dell'*International Production Orders Bill 2020* è disponibile al link:

Con la creazione di questo nuovo meccanismo di cooperazione, dovrebbe essere più semplice per le autorità britanniche accedere ai dati conservati al di fuori del proprio territorio e detenuti da fornitori di servizi con sede negli Stati Uniti.

Lo scopo dell'accordo, indicato all'art. 2, è promuovere la sicurezza pubblica e proteggere la privacy, le libertà nonché un internet aperto e liberamente accessibile, «*by resolving potential conflicts of legal obligations when communications service providers are served with Legal Process from one Party for the production or preservation of electronic data, where those providers may also be subject to the laws of the other Party*»⁸⁹⁹.

La dottrina ritiene che il nuovo accordo sia più vantaggioso per il Regno Unito, perché consentirà alle sue autorità giudiziarie di inviare ordine direttamente agli *internet service provider* statunitensi, superando le disposizioni di blocco dello *Stored Communications Act (SCA)*, che in passato impediva alle società di consegnare i dati memorizzati negli Stati Uniti alle forze dell'ordine straniera⁹⁰⁰.

13. I negoziati in vista di un Accordo tra l'Unione europea e gli Stati Uniti d'America

Gli Stati membri dell'Unione europea inviano un ingente numero di richieste di mutua assistenza aventi ad oggetto prove elettroniche agli Stati Uniti d'America, poiché ivi hanno sede i maggiori prestatori di servizi⁹⁰¹. Attualmente, tra l'Unione europea e gli Stati Uniti opera l'Accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, firmato il 25 giugno 2003⁹⁰². Nell'ambito dei principi delineati dall'Accordo, l'Italia e gli Stati Uniti d'America, il 3 maggio 2006, hanno firmato a Roma

https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6511_first-reps/toc_pdf/20025b01.pdf;fileType=application%2Fpdf.

⁸⁹⁹ Cfr., Art. 2, U.S.-UK Data Access Agreement.

⁹⁰⁰ Così, T. CHRISTAKIS, *21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)*, in *European Law Blog*, 13 ottobre 2019, p. 1 ss., disponibile al link: <https://europeanlawblog.eu/2019/10/17/21-thoughtsand-questions-about-the-uk-us-cloud-act-agreement-and-an-explanation-of-how-it-works-with-charts/>; N. KUSHWAHA, P. ROGUSKI, B.W. WATSON, *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*, cit., p. 51. Si veda anche J. DASKAL, P. SWIRE, *The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards*, in *Just Security*, 08 ottobre 2019, disponibile al link: <https://www.justsecurity.org/66507/the-ukus-cloud-act-agreement-is-finally-here-containing-new-safeguards/>.

⁹⁰¹ Un documento dell'Unione europea ha evidenziato come la cooperazione diretta su base volontaria tra Stati membri dell'UE e Stati Uniti d'America sia aumentata rapidamente, con più di 124000 richieste registrate nel 2017. Cfr., Raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione Europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale [COM (2019) 70 final]. Sul punto, anche M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 10.

⁹⁰² Cfr., Accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, in GUUE n. L 181 del 19 luglio 2003, p. 34 ss. L'Accordo è entrato in vigore il 1° febbraio 2010. Nel 2016 ha avuto luogo una revisione congiunta dell'Accordo. Durante i colloqui l'atto è stato ritenuto un valore aggiunto alla mutua assistenza giudiziaria, in quanto ha dimostrato di funzionare bene. Per il riesame, v., Riesame dell'accordo di assistenza giudiziaria UE-USA 2010, 7 aprile 2016, 7403/16, nonché GUUE L 336 del 10 dicembre 2016, p. 3 ss.

il Trattato di mutua assistenza in materia penale tra il Governo della Repubblica italiana e il Governo degli Stati Uniti d’America⁹⁰³.

Tuttavia, a causa dell’estrema volatilità e – più genericamente, “fragilità” – della prova elettronica, si è sviluppata, come valida alternativa alle tradizionali forme di cooperazione giudiziaria, la cooperazione diretta con i prestatori di servizi aventi sede negli Stati Uniti, basata sul trasferimento volontario dei soli dati non relativi al contenuto, nel rispetto della legislazione statunitense.

Ciò ha generato un’inevitabile ossidazione dei rapporti tra le autorità degli Stati membri dell’Unione europea e le autorità statunitensi a favore dell’espansione del campo di operatività dei privati, i quali sempre più occupano gli interstizi vuoti di tutela, lasciati liberi dall’assenza di una disciplina che dia risposte alle esigenze della nuova società digitalizzata. In altre parole, i prestatori di servizi hanno creato proprie strategie o decidono caso per caso se e in che modo cooperare. Ciò rende tale prassi inaffidabile e poco trasparente perché – tra le altre cose – non riuscirebbe a garantire un adeguato rispetto delle garanzie processuali.

Certezza giuridica, legittimità del procedimento penale, tutela dei diritti fondamentali per le persone coinvolte ed interessate, efficienza delle pratiche attuate: sono solo alcuni degli aspetti che possono far sorgere nel tecnico del diritto degli interrogativi – dei veri e propri dubbi – relativi alla bontà della cooperazione diretta con i privati su base volontaria⁹⁰⁴.

In tale contesto, è maturata la raccomandazione di decisione della Commissione dell’Unione europea di concludere un Accordo esecutivo come previsto dal CLOUD Act⁹⁰⁵, tant’è che una decisione del 21 maggio 2019, il Consiglio ha formalmente autorizzato la Commissione ad avviare i negoziati per un accordo tra l’Unione europea e gli Stati Uniti d’America⁹⁰⁶. Secondo la dottrina, il procedimento di negoziazione e conclusione dell’accordo non sarebbe facile, perché vi sarebbero profonde divergenze tra le Parti relative ai requisiti richiesti ed agli approcci sostenuti⁹⁰⁷.

Ciò nonostante, la Commissione sembra apparire salda nell’indicare come obiettivo da perseguire l’individuazione di «norme comuni per affrontare la questione giuridica

⁹⁰³ In Italia, il Trattato di mutua assistenza in materia penale tra il Governo della Repubblica italiana e il Governo degli Stati Uniti d’America è stato ratificato con l. 16 marzo 2009, n. 25. Il trattato è applicato dal 1° febbraio 2010.

⁹⁰⁴ Cfr., *Commission Impact Assessment accompanying the e-evidence package* (“Valutazione d’impatto della Commissione, che accompagna il pacchetto relativo alle prove elettroniche”, documento di lavoro disponibile in inglese), 17 aprile 2018, SWD(2018) 118 final.

⁹⁰⁵ Il riferimento è alla Raccomandazione di decisione del Consiglio che autorizza l’avvio di negoziati in vista di un Accordo tra l’Unione Europea e gli Stati Uniti d’America sull’accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale [COM (2019) 70 final]). Anche il Consiglio europeo, nelle conclusioni del 18 ottobre 2018, ha sottolineato l’importanza di tali questioni, precisando che «occorrerebbe trovare soluzioni per garantire un accesso transfrontaliero rapido ed efficiente alle prove elettroniche al fine di combattere efficacemente il terrorismo [...] ed altre forme gravi di criminalità, sia all’interno dell’UE che a livello internazionale entro la fine della legislatura si dovrebbe giungere a un accordo sulle proposte della Commissione riguardanti le prove elettroniche e l’accesso alle informazioni finanziarie, come pure su quella intesa a rendere più efficace la lotta al riciclaggio. La Commissione dovrebbe inoltre presentare con urgenza i mandati negoziali relativi ai negoziati internazionali sulle prove elettroniche».

⁹⁰⁶ Cfr., Decisione del Consiglio che autorizza l’avvio di negoziati in vista della conclusione di un accordo tra l’Unione europea e gli Stati Uniti d’America sull’accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale, 21 maggio 2019, 9114/19.

⁹⁰⁷ In tal senso, H.H. ABRAHA, *How compatible is the US ‘CLOUD Act’ with cloud computing? A brief analysis*, cit., p. 214.

specifica per l'accesso ai dati relativi al contenuto e a quelli non relativi al contenuto detenuti dai prestatori di servizi nell'Unione europea o negli Stati Uniti» nonché integrare «le proposte dell'UE riguardanti le prove elettroniche affrontando i conflitti di legge e rendendo più rapido l'accesso alle prove elettroniche»⁹⁰⁸.

L'Accordo con gli Stati Uniti consentirebbe una cooperazione diretta con un prestatore di servizi mediante la creazione di un quadro giuridico più efficace per le autorità giudiziarie. Invero, al momento attuale le autorità giudiziarie dei Paesi membri dell'Unione europea incontrano difficoltà per ottenere i dati relativi al contenuto attraverso richieste di assistenza giudiziaria.

La conclusione di un Accordo globale potrebbe fornire una maggiore chiarezza giuridica alle autorità giudiziarie e di contrasto di entrambe le Parti, perché consente, tra le altre cose, di evitare la facinorosa convivenza di norme profondamente diverse per i cittadini dell'Unione europea e i prestatori di servizi in base alla loro cittadinanza e sede.

Resta però da valutare come sarà possibile concludere un Accordo, dal momento in cui il CLOUD Act consente di certificare un “*foreign government*”, mentre l'Unione europea non sembra possedere tali caratteristiche.

Secondo alcuni studiosi statunitensi, all'espressione “*foreign government*” potrebbero attribuirsi due significati. La terminologia potrebbe far riferimento a un governo di un Paese straniero o ad una suddivisione politica di quel Paese⁹⁰⁹. In entrambi i casi, non potrebbe essere parte di un Accordo un'organizzazione internazionale come l'Unione europea, anche se *sui generis*. L'unico modo per rispettare la normativa statunitense sarebbe verificare dapprima che ogni Stato membro dell'Unione europea rispetti i requisiti previsti dal CLOUD Act⁹¹⁰.

Tuttavia, in una riunione del Comitato di coordinamento nel settore della cooperazione di polizia e giudiziaria in materia penale (CATS), tenutasi il 18 maggio 2018, la Commissione dell'Unione europea e il Servizio giuridico del Consiglio hanno chiarito che l'Unione europea è competente a condurre i negoziati con gli Stati Uniti e che gli Stati membri non dovrebbero avviare negoziati bilaterali⁹¹¹.

Dal nuovo accordo ci si attendono una serie di vantaggi pratici. Le norme dovrebbero fornire alle autorità giudiziarie l'accesso reciproco ai dati relativi al contenuto; risolvere delicate questioni relative all'accesso ai dati non relativi al contenuto sulla base di ordini emessi dalle autorità giudiziarie, in particolare per quanto riguarda l'accesso reciproco da parte delle autorità statunitensi, rivedendo le condizioni e le garanzie per una cooperazione diretta con i prestatori di servizi; contribuire a migliorare l'accesso tempestivo ai dati informatici da parte delle autorità giudiziarie; scongiurare il rischio di possibili conflitti di leggi; ridurre il rischio di frammentazione di norme e procedure nonché armonizzare i diritti e le garanzie tramite un unico mandato di negoziato per tutti

⁹⁰⁸ Così, testualmente, Raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione Europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale [COM (2019) 70 final]), p. 5.

⁹⁰⁹ Così, J. DASKAL, P. SWIRE, *A Possible EU-US Agreement on Law Enforcement Access to Data?*, in *Lawfare*, 21 maggio 2018, disponibile al link: <https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data>.

⁹¹⁰ Si potrebbe prevedere anche un Accordo quadro con l'Unione europea che stabilisca gli standard e risolva questioni di rilevanza per l'organizzazione e la successiva conclusione di specifici accordi con i singoli Stati membri. In tal senso, H.H. ABRAHA, *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, cit., p.151.

⁹¹¹ Cfr., *Dibattito orientativo sulle prove elettroniche del Consiglio dell'Unione europea*, Bruxelles, 28 maggio 2018, 9418/18, par. 8, p. 4.

gli Stati membri dell'UE con gli Stati Uniti, assicurando la non discriminazione tra gli Stati membri dell'Unione europea e i loro rispettivi cittadini; chiarire la natura vincolante e di esecuzione degli ordini per i prestatori di servizi, precisando al contempo gli obblighi per le autorità giudiziarie⁹¹².

Tuttavia, sarà necessario contemperare i vari interessi ed i vari diritti posti in gioco, in modo da ottenere un accettabile livello di tutela dei diritti fondamentali, che sia espressione concreta di un equilibrio tra esigenze proprie dell'autorità e garanzie di libertà. In tal senso, non può che divenire centrale la tutela dello Stato di diritto e della certezza del diritto, unici canoni ontologici che *de facto* potranno garantire la ragionevolezza e la proporzionalità delle scelte legislative da compiere e delle norme da applicare.

È evidente che l'Accordo dovrà rispettare il Regolamento (UE) 2016/679⁹¹³, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati⁹¹⁴, nonché le fonti di diritto primario dell'Unione europea, ponendo particolare attenzione ai diritti fondamentali, le libertà e i principi generali dell'Unione europea, tra cui vanno annoverati anche i diritti fondamentali garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, come sancito dall'art. 6, par. 3, TUE. I Trattati e la Carta dei diritti fondamentali dell'Unione europea non possono che rappresentare sicuro ed affidabile presidio di garanzia a tutela di tutte le persone, qualsiasi *status* esse assumano.

Se si tenesse conto della delicatezza della materia trattata, si noterebbe con estrema facilità come l'Accordo rischia di incidere profondamente su una serie di diritti delle persone fisiche ai cui dati è previsto l'accesso, dei prestatori di servizi e – più in generale e non per ultimi – del diritto alla libertà e alla sicurezza delle persone.

Regolare il trasferimento di dati informatici significa intervenire su principi e diritti delicati come la privacy e la protezione dei dati, il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, della libertà di espressione e di riunione, arrivando finanche a travolgere i diritti del e nel giusto processo penale, come il diritto di difesa, la presunzione di non colpevolezza, il principio di legalità e così via. Il rischio è quello di segnarli, graffiarli, scalfirli, rigarli, tagliarli e finanche reciderli, sino a ridurne la portata o annullarli del tutto.

Su un punto bisognerebbe convenire: i lavori per la negoziazione di un Accordo dovranno garantire il principio di non regressione dei diritti e la tutela dello Stato di diritto. Sarebbe inaccettabile compiere un passo indietro rispetto al livello di garanzia dei diritti sinora raggiunto.

⁹¹² Così, Raccomandazione di decisione del Consiglio che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione Europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale [COM (2019) 70 final]), p. 5 ss.

⁹¹³ Cfr., Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GUUE L 119 del 4 maggio 2016.

⁹¹⁴ Per delle note critiche sul rispetto del Regolamento GDPR da parte del CLOUD Act, H.H. ABRAHA, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, cit., p.213 ss.; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 2 ss.; J. SHURSON, *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, cit., p. 168 ss.

Per questi motivi, l'Unione europea non potrebbe concludere un Accordo internazionale la cui attuazione sarebbe contraria al diritto primario. Così come gli Stati Uniti non possono concludere un trattato che viola la Costituzione, nemmeno l'Unione può aderire a un accordo che viola, ad esempio, la Carta dei diritti fondamentali.

A tal proposito, appare interessante tener conto di quanto affermato di recente dalla Corte di giustizia dell'Unione europea⁹¹⁵. Secondo i giudici della Corte di Lussemburgo, gli Stati Uniti non offrono una protezione sufficiente ai dati trasferiti dall'Unione europea, perché non garantiscono un ricorso giurisdizionale effettivo⁹¹⁶ e non applicano il

⁹¹⁵ Cfr., Corte di giustizia, sentenza 16 luglio 2020, causa C-311/18, *Facebook Ireland Ltd. v Maximillian Schrems*. V., inoltre, H.H. ABRAHA, *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, cit., p.153; M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 9 ss. Per un approfondimento sulla sentenza *Schrems II*, C. BAARTMANS, M. COX, *De nasleep van Schrems II houdt niet over: de gevolgen van de uitspraak van het HvJ EU in Schrems II en de daaropvolgende (concept) aanbevelingen van de EDPD onder de loep genomen*, in *Mediaforum: Tijdschrift voor Media- en Communicatierecht*, 1, 2021, p. 2 ss.; F. D'ATH, *Arrêt «Schrems II»: sur la légalité des transferts de données personnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées*, in *Journal de droit européen*, 10, 2020, p. 442 ss.; M. DWORSCHAK, *Auswirkungen von Schrems II auf den Steuerdatentransfer*, in *Liechtensteinische Juristen-Zeitung*, 2020, p. 295 ss.; E. FLETT, J. WILSON, J. CLOVER, *Schrems strikes again: EU-US privacy shield suffers same fate as its predecessor*, in *Computer and Telecommunications Law Review*, 2020, p. 161 ss.; F. JACQUES, *«Uncle Sam is watching you» Retour sur les enseignements de l'arrêt Schrems II de la Cour de justice de l'Union européenne*, in *Journal des tribunaux*, 2021, p. 246 ss.; J.P. MELTZER, *After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals*, in *Global Privacy Law Review*, 1, 2021, p. 83 ss.; M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 3, 2020, p. 733 ss.; F. ROSSI DAL POZZO, *L'Accordo Privacy Shield non è un vero scudo per la privacy: scenari passati e futuri in merito al trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Rivista di diritto internazionale*, 4, 2020, p. 1112 ss.; M. ROTENBERG, *Schrems II, from Snowden to China: toward a new alignment on transatlantic data protection*, in *European Law Journal: review of European law in context*, 1-2, 2020, p.141 ss.; B. SANDFUCHS, *The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II*, in *Gewerblicher Rechtsschutz und Urheberrecht International*, 3, 2021 p. 245 ss.; C. SELLARS, *Schrems II and Standard Contractual Clauses – the Advocate-General's Opinion*, in *Computer Law Review International*, 1, 2020, p. 29 ss.; D. SIMON, *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l'invalidité du «bouclier de protection de la vie privée» à propos des transferts de données personnelles vers les États-Unis*, in *Europe: actualité du droit communautaire*, 8-9, 2020, p. 5 ss.; I. SOBRINO GARCÍA, *Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos*, in *Revista de Derecho Comunitario Europeo*, 68, 2021, p. 227 ss.; E. TEROLLI, *Privacy e protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza “Schrems II”*, in *Il diritto dell'informazione e dell'informatica*, 1, 2021, p. 49 ss.; C. THIELE, *Ist der Datentransfer in die USA am Ende? - Zur Unzulässigerklärung des EU Privacy Shield - Analyse der Entscheidung EuGH 16. 7. 2020, C-311/18 mit Praxistipps*, in *JusIT, IT-Recht, Rechtsinformation, Datenschutz*, 70, 2020, p. 196 ss.; X. TRACOL, *Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations*, in *ERA Forum*, 4 agosto 2021, disponibile al link: <https://link.springer.com/article/10.1007/s12027-021-00679-1>; ID., *“Schrems II”: the return of the privacy shield*, in *Computer law & security review*, 39, 2020, p. 1 ss.

⁹¹⁶ Sul punto, Corte di giustizia, sentenza 16 luglio 2020, causa C-311/18, *Facebook Ireland Ltd. v Maximillian Schrems*, pt. 191, 192, 193 e 197, secondo cui «La Commissione rileva, al punto 115 della decisione “scudo per la privacy”, che “sebbene la persona, compreso l'interessato dell'[Unione], sottoposta a sorveglianza (elettronica) illecita per finalità di sicurezza nazionale disponga di una serie di possibilità di ricorso, altrettanto pacifico è che queste non contemplano almeno alcune delle basi giuridiche di cui possono avvalersi le autorità di intelligence statunitensi (ad esempio l'EO 12333)”. Pertanto, riguardo all'E.O. 12333, in tale punto 115 essa ha sottolineato la mancanza di qualsiasi mezzo di ricorso, Orbene, secondo la giurisprudenza ricordata al punto 187 della presente sentenza, una lacuna siffatta nella tutela

principio di proporzionalità⁹¹⁷, garantendo un livello di tutela pari a quanto previsto dalla Carta dei diritti fondamentali dell'UE, nei programmi di sorveglianza e, più in generale, nelle questioni relative alla tutela della privacy⁹¹⁸.

giurisdizionale rispetto alle ingerenze collegate ai programmi di intelligence basati su tale decreto presidenziale osta a che si concluda – come ha fatto la Commissione nella decisione “scudo per la privacy” – che il diritto degli Stati Uniti garantisce un livello di protezione sostanzialmente equivalente a quello garantito dall'articolo 47 della Carta.

Inoltre, per quanto riguarda tanto i programmi di sorveglianza fondati sull'articolo 702 del FISA, quanto quelli fondati sull'E.O. 12333, è stato rilevato ai punti 181 e 182 della presente sentenza, che né la PPD-28 né l'E.O. 12333 conferiscono agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici, cosicché tali interessati non dispongono di un diritto di ricorso effettivo.

Ai punti 115 e 116 della decisione “scudo per la privacy”, tuttavia, la Commissione ha constatato che per effetto dell'esistenza del meccanismo di mediazione istituito dalle autorità statunitensi – quale descritto nella lettera inviata il 7 luglio 2016 dal Segretario di Stato statunitense alla Commissaria europea per la Giustizia, i Consumatori e la parità di genere, contenuta all'allegato III di tale decisione – e della natura della missione affidata al Mediatore, ossia quella di “Primo coordinatore della diplomazia internazionale per le tecnologie dell'informazione”, si poteva considerare che gli Stati Uniti assicurano un livello di protezione sostanzialmente equivalente a quello garantito all'articolo 47 della Carta.

[...]

Pertanto, il meccanismo di mediazione di cui alla decisione “scudo per la privacy” non fornisce mezzi di ricorso dinanzi a un organo che offra alle persone i cui dati sono trasferiti verso gli Stati Uniti garanzie sostanzialmente equivalenti a quelle richieste dall'articolo 47 della Carta».

⁹¹⁷ Cfr., Corte di giustizia, sentenza 16 luglio 2020, causa C-311/18, *Facebook Ireland Ltd. v Maximillian Schrems*, pt. 180 e 181, secondo cui «Appare quindi che l'articolo 702 del FISA non fa emergere in alcun modo l'esistenza di limitazioni all'autorizzazione che esso comporta per l'attuazione dei programmi di sorveglianza ai fini dell'intelligence esterna, né l'esistenza di garanzie per i cittadini stranieri potenzialmente oggetto di tali programmi. In tali circostanze, e come sostanzialmente rilevato dall'avvocato generale ai paragrafi 291, 292 e 297 delle sue conclusioni, tale articolo non è idoneo a garantire un livello di tutela sostanzialmente equivalente a quello garantito dalla Carta, come interpretata dalla giurisprudenza ricordata ai punti 175 e 176 della presente sentenza, secondo cui, per soddisfare il principio di proporzionalità, una base giuridica che consente ingerenze nei diritti fondamentali deve definire essa stessa la portata della limitazione dell'esercizio del diritto di cui trattasi e prevedere norme chiare e precise che regolino la portata e l'applicazione della misura e impongano requisiti minimi.

In base alle constatazioni contenute nella decisione “scudo per la privacy”, è vero che i programmi di sorveglianza fondati sull'articolo 702 del FISA devono essere attuati nel rispetto dei requisiti risultanti dalla PPD-28. Tuttavia, sebbene la Commissione abbia sottolineato, ai punti 69 e 77 della decisione «scudo per la privacy, che siffatti requisiti sono vincolanti per i servizi di intelligence statunitensi, il governo degli Stati Uniti ha ammesso, in risposta ad un quesito della Corte, che la PPD-28 non conferisce agli interessati diritti nei confronti delle autorità statunitensi azionabili dinanzi ai giudici. Pertanto, essa non è idonea a garantire un livello di protezione sostanzialmente equivalente a quello risultante dalla Carta, contrariamente a quanto richiesto dall'articolo 45, paragrafo 2, lettera a), del RGPD, secondo il quale la constatazione di tale livello dipende, in particolare, dall'esistenza dei diritti effettivi e azionabili di cui godono le persone i cui dati sono stati trasferiti verso il paese terzo di cui trattasi».

⁹¹⁸ Sulle questioni cruciali che si dovranno affrontare in sede di formazione dell'Accordo, particolarmente interessante potrebbe essere un Parere della Corte di Giustizia dell'Unione europea espresso per la bozza di Accordo tra Unione europea e Canada sullo scambio di informazioni di passeggeri aerei (i cc.dd. PNR). In particolare, i giudici hanno fatto notare che l'accordo non contenesse una dettagliata regolamentazione relativa ai dati trasferiti, ed in particolare ai dati sensibili. Inoltre, l'Accordo risultava contenere vincoli alla conservazione dei dati del tutto insufficienti rispetto alle esigenze ed ai diritti da garantire e non individuava nessuna restrizione all'uso dei dati trasferiti. Cfr., Corte di giustizia, parere 26 luglio 2017, C-1/15, *Progetto di accordo tra il Canada e l'Unione europea – Trasferimento dei dati del codice di prenotazione dei passeggeri aerei dall'Unione al Canada*. Sul parere, in dottrina, P. BEAUVAIS, M. BENLOLO-CARABOT, *Droit pénal de l'Union européenne*, in *Revue trimestrielle de droit européen*, 4, 2017, p.884 ss.; C. BILLET, *Une nouvelle revendication de l'autonomie de l'ordre juridique de l'Union européenne: (CJUE, avis 1/15 du 26 juillet 2017, projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement des données des dossiers passagers)*, in AA.VV., *Annuaire français de droit*

Per questo, la stessa Commissione ha richiesto che l'Accordo tenga conto del principio di necessità e proporzionalità, della tutela dei diritti fondamentali e della disponibilità di meccanismi di tutela giurisdizionale per gli interessati⁹¹⁹.

Queste riflessioni fanno emergere, quale corollario, altre questioni di pari rilevanza ed assolutamente centrali per la chiarezza e precisione applicativa del futuro Accordo.

L'ordinamento statunitense, già da tempo, ha la tendenza ad operare una forte *vis espansiva* della propria giurisdizione al di fuori dei propri confini⁹²⁰, coinvolgendo anche soggetti – persone fisiche e giuridiche – dell'Unione europea. Diventa assolutamente essenziale affrontare il tema dell'extraterritorialità.

Ad esempio, gli Stati Uniti hanno imposto vari tipi di sanzioni economiche nei confronti di Stati e di individui o entità giuridiche⁹²¹. Orbene, le sanzioni non si rivolgono

international, LXIII/2017, Parigi, 2018, p. 429 ss.; C. DOCKSEY, *Opinion 1/15 Privacy and security, finding the balance*, in *Maastricht Journal of European and Comparative Law*, 6, 2017, p. 768 ss.; J. EYNARD, *D'une ingérence généralisée à une autre: deux poids, deux mesures?*, in *Revue trimestrielle des droits de l'homme*, 11, 2018 p.761 ss.; C. FORGET, *L'avis de la C.J.U.E. sur l'accord PNR Union européenne-Canada: une occasion ratée de réaffirmer le principe de finalité?*, in *Journal de droit européen*, 247, 2018, p.87 ss.; E. GUILD, E. MENDOS KUŞKONMAZ, *A critical take on opinion 1/15: is the glass half full or half empty?*, in AA.VV., *European yearbook on human rights* (P. CZECH, L. HESCHL, K. LUKAS, M. NOWAK, G. OBERLEITNEIR eds.), Cambridge, 2019, p. 111 ss.; EAD., *EU Exclusive jurisdiction on surveillance related to terrorism and serious transnational crime: case review on opinion 1/15*, in *European Law Review*, 4, 2018, p. 583 ss.; H. HIJMANS, *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, in *European Data Protection Law Review*, 3, 2017, p. 406 ss.; C. KUNER, *International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 3, 2018, p.857 ss.; N. LE BONNIEC, *L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne: une délicate conciliation entre sécurité nationale et sécurité numérique*, in *Revue trimestrielle de droit européen*, 3, 2018, p. 617 ss.; V.M. PFISTERER, *The Right to Privacy-A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, in *German Law Journal*, 5, 2019, p. 722 ss.; R. POMAHÁČ, *Soudní dvůr EU: Předávání údajů jmenné evidence cestujících v letecké dopravě z Unie do Kanady*, in *Právní rozhledy: časopis pro všechna právní odvětví*, 21, 2017, p. 761 ss.; R. PRIEBE, *EuGH beanstandet Fluggastdatenabkommen zwischen der EU und Kanada*, in *Europäische Zeitschrift für Wirtschaftsrecht*, 19, 2017, p.762 ss.; E.A. ROSSI, *Gli accordi PNR (Passenger Name Record) nella lotta al terrorismo internazionale. Conseguenze del parere n. 1/15 della Corte di giustizia del 26 luglio 2017 per la legittimità della direttiva n. 2016/681/UE*, in *Diritto comunitario e degli scambi internazionali*, 3, 2018 p. 395 ss.; D. SIMON, *Applicabilité des accords entre l'Union européenne et le Royaume du Maroc au territoire du Sahara occidental: Acte II*, in *Europe*, 4, 2018, p. 6 ss.; X. TRACOL, *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record Data between the EU and Canada*, in *Computer Law & Security Review*, 34, 2018, p. 830 ss.; V. TZORTZI, *I shediazomeni symfonia PNR-EE-Kanatha paraviazei ta themeliodi dikaionomata: paratiriseis*, in *Elliniki Epitheorisi Evropaikou Dikaion*, 2017, p. 461 ss.; A. VEDASCHI, *The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15 The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15*, in *European Constitutional Law Review*, 14, 2018, p. 410 ss.; M. ZALNIERIUTE, *Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *The Modern Law Review*, 6, 2018, p. 1046 ss.

⁹¹⁹ In tal senso, M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, cit., p. 11.

⁹²⁰ In una nota *dissenting opinion*, il giudice J. Brennan, nella causa *Stati Uniti v. Verdugo-Urquidez* del 1990 affermò che: «l'enorme espansione della giurisdizione penale federale al di fuori dei confini della nostra Nazione ha indotto un autore a suggerire che i tre prodotti maggiormente esportati dal nostro paese siano oggi il rock, i blue jeans e il diritto statunitense». Tale pensiero era già presente in V.R. GRUNDMAN, *The New Imperialism: The Extraterritorial Application of United States Law*, in *The International Lawyer*, 14, 1980, p. 257. Per un approfondimento, B. REDDING, *The Long Arm of the Law or the Invasive Reach of the American Legal System*, in *International Business Law Journal*, 5, 2007, p. 659.

⁹²¹ Alcune di queste sanzioni sono di lunga data, come l'embargo contro Cuba, autorizzato dal *Foreign Assistance Act* (legge sull'assistenza estera) del 1961 e codificato, nel 1996, dal *Cuban Liberty and*

solo a soggetti statunitensi e non statunitensi sottoposti alla giurisdizione degli Stati Uniti, ma gran parte della legislazione statunitense che attua tali sanzioni mira a sanzionare entità di Stati terzi che effettuino scambi commerciali con lo Stato interessato oppure a vietare a tali entità, a loro volta, di commerciare con gli Stati Uniti.

In tale contesto, con riferimento alla privacy, bisogna riflettere su quanto affermato dall'avvocato generale Hogan nelle proprie conclusioni al caso *Bank Mellî*, il quale ritiene che «le sfide che l'extraterritorialità di talune normative pone al diritto dell'Unione dovrebbero manifestarsi con una certa intensità, negli anni a venire, anche in un settore caro alla Corte, ossia quello della protezione dei dati personali. Infatti, il *Clarifying Lawful Overseas Use of Data Act* del 2018 degli Stati Uniti (legge recante chiarimento sull'utilizzo legittimo di dati all'estero), che ha modificato lo *Stored Communications Act* del 1986 (legge sulle comunicazioni archiviate), attribuisce alle autorità statunitensi preposte all'applicazione della legge il potere di richiedere i dati archiviati dalla maggior parte dei principali fornitori di servizi di cloud, anche se conservati al di fuori degli Stati Uniti. Tuttavia, il mercato dell'archiviazione dei dati è ampiamente dominato da società statunitensi, in misura superiore all'85%»⁹²².

Invero, i tentativi di esercitare una giurisdizione extraterritoriale sono stati tradizionalmente criticati dall'Unione europea, perché costituiscono una forma di giurisdizione sproporzionata, difficilmente conciliabile con i principi generali del diritto internazionale pubblico.

È da qui che bisognerà partire per comprendere quale possa essere la soluzione migliore, soprattutto in applicazione delle disposizioni generali sull'azione estera e sulla politica estera previsti all'art. 21, par. 1 e par. 2, lett. h), TUE, volte a promuovere, tra le altre cose, un sistema internazionale basato su una cooperazione multilaterale rafforzata e il buon governo mondiale al fine di garantire la democrazia, lo Stato di diritto, l'universalità e indivisibilità dei diritti dell'uomo e delle libertà fondamentali, il rispetto della dignità umana, i principi della Carta delle Nazioni Unite e dei diritti internazionali⁹²³.

Se da una parte l'Unione europea è coinvolta nello sviluppo di nuovi strumenti per l'acquisizione dell'*e-evidence* basati sul principio della mutua assistenza che coinvolgono i rapporti con Stati terzi, dall'altra, sta creando una nuova disciplina che si affianca

Democratic Solidarity Act (legge per la libertà e la solidarietà democratica a Cuba, o legge *Libertad*). Dall'11 settembre 2001, con l'intensificarsi della lotta contro il terrorismo, il programma statunitense di sanzioni economiche è stato ampliato.

⁹²² V., Conclusioni dell'Avvocato generale Gerard Hogan presentate il 12 maggio 2021, causa C-124/20, *Bank Mellî Iran, Aktiengesellschaft nach iranischem Recht c. Telekom Deutschland GmbH*.

⁹²³ L'art. 21, TUE, recita: «1. L'azione dell'Unione sulla scena internazionale si fonda sui principi che ne hanno informato la creazione, lo sviluppo e l'allargamento e che essa si prefigge di promuovere nel resto del mondo: democrazia, Stato di diritto, universalità e indivisibilità dei diritti dell'uomo e delle libertà fondamentali, rispetto della dignità umana, principi di uguaglianza e di solidarietà e rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale.

L'Unione si adopera per sviluppare relazioni e istituire partenariati con i paesi terzi e con le organizzazioni internazionali, regionali o mondiali, che condividono i principi di cui al primo comma. Essa promuove soluzioni multilaterali ai problemi comuni, in particolare nell'ambito delle Nazioni Unite.

2. L'Unione definisce e attua politiche comuni e azioni e opera per assicurare un elevato livello di cooperazione in tutti i settori delle relazioni internazionali al fine di:

[...]

h) promuovere un sistema internazionale basato su una cooperazione multilaterale rafforzata e il buon governo mondiale».

all'ordine europeo di indagine per la formazione delle prove elettroniche transnazionali, la cui base giuridica è rappresentata dall'art. 82, par. 1, TFUE.

I nuovi ordini europei di produzione e di conservazione, basati sul principio del mutuo riconoscimento, dovranno essere più efficienti rispetto ai vecchi strumenti del passato e prevedere un ampio livello di garanzie dei diritti fondamentali, nel pieno rispetto di quanto previsto dalla Carta dei diritti fondamentali dell'Unione europea, così come interpretata dalla Corte di giustizia, dalle tradizioni costituzionali comuni e dalla Convenzione europea dei diritti dell'uomo.

L'analisi della disciplina, dunque, consentirà di verificare come si stia sviluppando un rapporto diretto tra autorità pubbliche e società private presenti in altri Stati membri e di appurare l'evoluzione della cooperazione giudiziaria in materia penale nel campo dell'acquisizione delle prove elettroniche transnazionali.

CAP. III – LA CONVENZIONE EUROPEA SULLA CRIMINALITÀ INFORMATICA E LA
COOPERAZIONE CON GLI USA

CAPITOLO IV

MUTUO RICONOSCIMENTO E LEGALE FORMAZIONE DELL'*E-EVIDENCE*

Sommario: 1. La necessità di strumenti all'avanguardia per la legale formazione della prova elettronica transnazionale nell'Unione europea. – 2. L'ordine europeo di indagine avente ad oggetto la prova elettronica. 3. L'inadeguatezza dell'ordine europeo di indagine: verso una disciplina dell'*e-evidence* transfrontaliera nello spazio di libertà, sicurezza e giustizia. – 4. Gli ordini europei di produzione e conservazione: la scelta della fonte normativa. – 5. La funzione e l'ambito di applicazione degli ordini europei di produzione e conservazione. – 6. L'ordine europeo di conservazione. – 7. L'ordine europeo di produzione. – 7.1. (Segue). La procedura di riesame in caso di contrasto con il diritto di un Paese terzo. – 8. L'intervento dell'autorità di esecuzione in caso di inottemperanza. – 9. Il principio del “diritto a difendersi, ricorrendo effettivamente”.

1. La necessità di strumenti all'avanguardia per la legale formazione della prova elettronica transnazionale nell'Unione europea

Come si è avuto modo di chiarire, intorno alla prova elettronica transnazionale ruotano un fascio di problematiche ancora irrisolte, che richiedono scelte politiche importati, inserite nel più ampio contesto della tutela dei diritti fondamentali coinvolti.

Una prima importante risposta è stata data dal Consiglio d'Europa e dagli Stati Uniti che, con modalità e metodologie differenti, hanno deciso di affrontare il problema con un approccio pragmatico, ma la cui efficienza va verificata sul campo e nel tempo.

Nell'ambito più ristretto dell'Unione europea, sicuramente caratterizzato da un livello più elevato di fiducia reciproca, è iniziato un cammino di condivisione e di scambio di opinioni, finalizzato alla creazione di nuovi strumenti più efficaci per la legale formazione della prova elettronica.

Non si vuol dire che in tale ordinamento non esistano strumenti idonei alla formazione della prova elettronica. Piuttosto, si è consapevoli che gli strumenti attualmente esistenti non riescono in modo efficace e rapido a formare le prove elettroniche necessarie per i procedimenti penali.

Tale necessità è apparsa lampante con il crescere del numero di procedimenti penali relativi a qualsiasi tipo di reato in cui le autorità degli Stati membri richiedono l'accesso ai dati che potrebbero servire da elementi aventi attitudine probatoria e che sono conservati al di fuori del loro Paese o da prestatori di servizi situati in altri Stati membri o in Paesi terzi⁹²⁴.

In effetti, l'efficacia delle indagini e dei procedimenti penali nell'Unione europea è attualmente ostacolata dalla difficoltà nell'accesso transfrontaliero alle prove elettroniche, a causa di una perdurante mancanza di efficienza nella cooperazione

⁹²⁴ Cfr., *Relazione* alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, COM(2018) 225 final, p. 1.

giudiziaria tra autorità pubbliche, nella cooperazione diretta tra autorità pubbliche e prestatori di servizi, e nell'accesso diretto delle autorità pubbliche alle prove elettroniche. Pertanto, le indagini si bloccano, i reati restano impuniti, le vittime sono meno tutelate e tra i cittadini si diffonde la percezione di un abbassamento del livello di sicurezza⁹²⁵.

Come il Consiglio d'Europa e, in parte, gli Stati Uniti d'America, anche l'Unione europea ha ritenuto di avviare un nuovo *iter* per la creazione di nuovi strumenti che consentissero alle autorità del singolo Stato membro di richiedere direttamente i dati elettronici ad un *internet service provider* con sede in un altro Stato membro o in un Paese terzo, senza il preventivo confronto con l'autorità pubblica in cui ha sede il privato detentore del dato richiesto.

Tale soluzione – invero ricca di aspetti tanto risolutivi quanto problematici – comporta, secondo alcuni, quale corollario il preoccupante difetto di affidare all'azienda privata detentrica del dato il controllo sull'eseguibilità degli ordini⁹²⁶.

Tuttavia (ed in ciò si manifesta tutto l'annoso dilemma che attanaglia le riflessioni dei giuristi e dei tecnici del settore) l'obiettivo di rendere più efficaci le indagini ed i processi penali, migliorando l'accesso transfrontaliero alle prove elettroniche, mediante la riduzione dei tempi e idonee garanzie di accesso nei casi in cui attualmente manca, comporta l'indispensabile rinnovamento degli strumenti e l'urgenza di agire, pur nel rispetto del dettato delle fonti che individuano – talvolta in maniera esplicita, talaltra in modo implicito – i diritti fondamentali posti a tutela della persona umana, garantendo al tempo stesso certezza del diritto, trasparenza e responsabilità degli attori che calcano il proscenio⁹²⁷ della procedura penale europea.

L'utilità di strumenti all'avanguardia per ottenere l'accesso transfrontaliero ai dati è particolarmente rilevante poiché i moderni mezzi digitali consentono l'efficace lotta contro il terrorismo, la criminalità informatica e la criminalità transnazionale nella sua interezza⁹²⁸.

Non che all'Unione europea manchino strumenti recentemente creati per la formazione della prova transnazionale ovvero che non esistano convenzioni sull'assistenza giudiziaria con procedure *in rem* snelle nel caso in cui l'oggetto sia una prova elettronica, bensì si vuole rimarcare l'indiscussa necessità per gli organismi dell'Unione di creare un nuovo assetto in grado di rendere tempestive le attività di ricerca

⁹²⁵ Tale problematica è evidenziata nel Documento di lavoro dei servizi della Commissione “*Sintesi della valutazione d'impatto*” che accompagna il documento “Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale” e “Proposta di direttiva del Parlamento europeo e del Consiglio che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali”, del 17 aprile 2018, SWD(2018) 119 final.

⁹²⁶ Su tali criticità, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1288.

⁹²⁷ Il parallelismo tra processo e teatro è cosa nota in letteratura e nella sociologia. Il *trait d'union* tra i due fenomeni è ravvisabile proprio nel concetto di rappresentazione. Si è parlato di antica complicità tra processo e teatro come anche di processo penale quale rappresentazione sacra in cui il delitto è punito in effigie mediante le forme teatrali. Per tali riflessioni, E. AMODIO, *Il processo come gioco tra letteratura e diritto vivente*, cit., p. 1664 ss.; M. ASCOLI, *La interpretazione delle leggi*, Roma, 1928, p. 24; M. CARTABIA, L. VIOLANTE, *Teatro e processo penale*, in M. CARTABIA, L. VIOLANTE, *Giustizia e mito*, Bologna, 2018, p. 145 ss.; G. SOULIER, *Le théâtre et le procès*, in *Droit et société*, (117/118), 1991, p. 8. Si consultino, inoltre, gli scritti raccolti nel volume *Représentations du procès. Droit, théâtre, littérature, cinéma*, diretto da C. BIET e L. SCHIFANO, Parigi, 2003.

⁹²⁸ In tal senso, A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, in *Eucrim*, 1, 2020, p. 46.

e trasferimento dei dati elettronici disseminati sul territorio europeo o in possesso di *internet service provider* con sede in uno Stato membro ed utili in un processo penale.

In effetti, vi sono già fonti normative vigenti nello spazio di libertà, sicurezza e giustizia che consentono l'attivazione di procedure volte alla formazione delle prove. Nonostante ciò, il quadro degli strumenti di cooperazione investigativa o probatoria adottabili appare incompleto.

Non sembrava riuscire a garantire il raggiungimento degli obiettivi indicati la decisione quadro 2008/978/GAI in tema di mandato europeo di ricerca della prova (M.E.R.)⁹²⁹. Non si può considerare soddisfacente neanche la Convenzione europea di

⁹²⁹ In GUUE L-350, del 30 dicembre 2008, p. 72 ss. La decisione quadro in esame non è mai stata trasposta dall'ordinamento italiano, che, con lungimiranza, aveva compreso che lo strumento fosse del tutto inefficace a causa del suo ridotto campo applicativo, siccome poteva esser utilizzato solo per acquisire oggetti, documenti o dati reperibili in altri Stati. Anche altri Stati, come Austria e Svezia, non hanno recepito la decisione quadro. Lo strumento ha, dunque, avuto vita breve, poiché praticamente quasi da subito si parlò della sostituzione di esso con un mezzo più moderno ed efficiente. Infatti, lo strumento si è rivelato sostanzialmente inefficace a causa del suo ridotto ambito applicativo. La decisione quadro viene dapprima sostituita dalla direttiva 2014/41/UE relativa all'ordine europeo di indagine penale e poi abrogata con Reg.(UE) n. 95/2016 del Parlamento europeo e del Consiglio del 20 gennaio 2016 in GUUE L-26/9 del 2 febbraio 2016. Nonostante sin da subito lo strumento si sia rivelato inefficace, data la sua portata innovativa, la bibliografia sul tema è alquanto ampia. Sull'argomento, *ex multis*, si legga E. BARBE, *La coopération judiciaire en matière pénale au sein de l'Union Européenne: les voies incertaines de la reconnaissance mutuelle*, in AA.VV., *La protection des intérêts financiers de l'Union et le rôle de l'Olaf vis-à-vis de la responsabilité pénale des personnes morales et des chefs d'entreprises et admissibilité mutuelle des preuves (Acts des Journées d'études de Inverigo – Como)* (a cura di F. RUGGIERI), Bruylant, Bruxelles, 2005, p. 105 ss.; R. BELFIORE, *La prova penale "raccolta" all'estero*, Roma, 2014, p. 197 ss.; ID., *Movement of Evidence in the EU: The Present Scenario and Possible Future Developments*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 17, 2009, p. 2 ss.; ID., *Il mandato europeo di ricerca delle prove e l'assistenza giudiziaria nell'Unione europea*, in *Cass. pen.*, 10, 2008, p. 3894 ss.; M. DANIELE, *Ricerca e formazione della prova*, Sezione I – *Profili generali*, in AA.VV., *Manuale di procedura penale europea*, (a cura di R.E. KOSTORIS), III ediz., Padova, 2019, p. 455 ss.; G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., *«Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), cit., p. 569 ss.; ID., *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), cit., p. 1173 ss.; G. DE AMICIS, *Il mandato europeo di ricerca delle prove: un'introduzione*, in *Cass. pen.*, 7/8, 2008, p. 3033 ss.; ID., *Limiti e prospettive del mandato europeo di ricerca della prova*, in *penalecontemporaneo.it*, 5 aprile 2011, p. 10 ss., disponibile al link: <https://archiviopdc.dirittopenaleuomo.org/d/500-limiti-e-prospettive-del-mandato-europeo-di-ricerca-della-prova>; P. DE HERT, K. WEIS, N. CLOOSEN, *The Framework Decision of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for use in Proceedings in Criminal Matters – A Critical Assessment*, in *New Journal of European Criminal Law*, 2009, p. 55 ss.; B. HECKER, *Mutual recognition and Transfer of Evidence. The European Evidence Warrant*, in AA.VV., *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (a cura di S. RUGGERI), cit., p. 269 ss.; L. KLIMEK, *Free movement of evidence in criminal matters in the EU*, in *The Lawyer Quarterly*, 4, 2012, p. 265 ss.; R.E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, cit., p. 1177 ss.; E.N. LA ROCCA, *Dalla "libera circolazione dei soggetti" alla "libera circolazione del materiale probatorio": la Decisione-Quadro sul mandato europeo di ricerca delle prove*, in *Osservatorio del processo penale*, 2007, p. 37 ss.; A. MANGIARACINA, *La circolazione della prova dichiarativa in ambito nazionale ed europeo*, in *Giust. Pen.*, 3, 2010, p. 443 ss.; M.R. MARCHETTI, *Dalla Convenzione di assistenza giudiziaria in materia penale nell'Unione europea al mandato europeo di ricerca delle prove e all'ordine europeo di indagine penale*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), cit., p. 150 ss.; ID., *Il mandato europeo di ricerca delle prove*, in *Studi in onore di Mario Pisani*, vol. II, *Diritto processuale penale e profili internazionali. Diritto straniero e diritto comparato* (a cura di P. CONSO, E. ZANETTI), Piacenza, 2010, p. 369 ss.; ID., *L'assistenza giudiziaria internazionale*, in AA.VV., *Trattato di procedura penale* (diretto da G. UBERTIS, G.P. VOENA), cit., p. 23

assistenza giudiziaria del 2000⁹³⁰, che pur fa riferimento a modelli per la legale formazione di prove transfrontaliere di nuova generazione. Scarsamente rilevanti sono gli

ss.; O. MAZZA, *Il principio del mutuo riconoscimento nella giustizia penale, la mancata armonizzazione e il mito taumaturgico della giurisprudenza europea*, in ID., *Il garantismo al tempo del giusto processo*, cit., p. 63 ss.; G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, cit., p. 268 ss.; M. MENNA, *Mandato di ricerca della prova e sistemi probatori*, in *Dir. pen. proc.*, 3, 2011, p. 370 ss.; V. MITSILEGAS, *EU Criminal Law*, London, 2009; C.C. MURPHY, *The European Evidence Warrant: mutual recognition and mutual (dis)trust?*, in AA.VV., *Crime within the area of Freedom, Security and Justice. A European Public Order* (a cura di C. ECKES, T. KONSTADINIDES), Cambridge, 2011, p. 224 ss.; N. PARISI, *Il mandato europeo di ricerca delle prove nel sistema della cooperazione giudiziaria penale fra gli Stati membri dell'Unione*, in *Riv. it. dir. inter. Priv. e proc.*, 2, 2009, p. 327 ss.; A. PERDUCA, *Prove, investigazioni e cooperazione giudiziaria su scala europea*, in AA.VV., *Processo penale e giustizia europea. Omaggio a Giovanni Conso*, Milano, 2010, p. 479 ss.; M. PISANI, *La decisione quadro sul mandato europeo di ricerca delle prove*, in *Riv. it. Dir. proc. pen.*, 1, 2009, p. 479 ss.; J.A.E. VERVAELE, *Il progetto di decisione quadro sul mandato di ricerca della prova*, in AA.VV., *Prova penale e Unione europea, Atti del Convegno "L'armonizzazione della prova penale nell'Unione europea". Facoltà di Giurisprudenza dell'Università di Bologna. 18-19 aprile 2008* (a cura di G. ILLUMINATI), Bologna, 2009, p. 153 ss.; C. WILLIAMS, *The european Evidence Warrant: the proposal of the European Commission*, in AA.VV., *Dealing with european evidence in criminal proceedings: national practice and European Union policy* (Proceedings of ERA /Crown Prosecution Service Conference – AGIS Project), 18-20 novembre 2004, ERA – Forum, Trier, 2005, p. 17 ss.;

⁹³⁰ La Convenzione europea di assistenza giudiziaria, firmata a Bruxelles il 29 maggio 2000, è stata pubblicata in GUCE C-197 del 12 luglio 2000 ed è entrata in vigore il 23 agosto 2005. L'Italia ha dato attuazione alla Convenzione con il d.lgs. 5 aprile 2017, n. 52, in GU n. 97 del 24 aprile 2017. La Convenzione di Bruxelles si caratterizza per un innovativo sistema di cooperazione giudiziaria rispetto alla Convenzione di Strasburgo del 1959, ma è stata superata dalla direttiva 2014/41/UE, che la sostituisce in molte parti. In particolare, la Convenzione di Bruxelles del 2000 continua ad operare per i fenomeni non regolati dalla direttiva 2014/41/UE, in relazione alle notificazioni o ai rapporti tra autorità amministrative, e *in toto* nelle relazioni con gli Stati che non hanno aderito alla direttiva sull'ordine europeo di indagine penale, come la Danimarca e l'Irlanda.

L'elemento di assoluta differenza con la Convenzione di Strasburgo del 1959 sta nella rivisitazione del metodo intergovernativo che si caratterizza per la quasi totale eliminazione del filtro politico del Ministro della giustizia, poiché si consente un diretto contatto tra autorità giudiziarie e si relega ai soli casi di eccezionalità l'intermediazione del Guardasigilli. L'obiettivo era quello di creare uno strumento più funzionale ed efficace alla lotta alla criminalità transnazionale, attraverso la riduzione dei tempi e la importante diminuzione dei rischi di un mancato esperimento dello strumento di assistenza giudiziaria per ragioni strettamente politiche, incentivando la fiducia tra Stati e tra autorità giudiziarie, elemento necessario per costruire uno spazio giudiziario europeo comune, in linea con quanto stabilito dal Trattato di Amsterdam e dal Consiglio di Tampere. Sulla Convenzione, E. ANODINA, *Cooperazione-integrazione penale nell'Unione Europea*, in *Cass. pen.*, 10, 2001, p. 2898 ss.; E. CALVANESE, G. DE AMICIS, *Appunti sulla Nuova Convenzione di assistenza giudiziaria penale tra gli Stati membri dell'Unione europea*, in *Giur. Merito*, 4-5, 2000, p. 1052 ss.; L. CAMALDO, *L'attuazione della Convenzione di Bruxelles del 2000: l'assistenza giudiziaria in materia penale assume una configurazione a "geografia variabile"*, in *penalecontemporaneo.it*, 19 luglio 2017; L. CAMALDO, F. MANFREDINI, *La cooperazione giudiziaria nell'era delle minacce globali e la riforma del Libro XI del codice di procedura penale*, cit., p. 3043 ss.; G. DARAIO, *Le rogatorie*, cit., p. 1080; B. GALGANI, *Assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 444 ss.; E.N. LA ROCCA, *La legge di ratifica ed esecuzione della Convenzione di assistenza giudiziaria in materia penale tra gli Stati membri Ue*, in *Arch. pen.*, 3, 2016, p. 1 ss.; M.R. MARCHETTI, *Dalla Convenzione di assistenza giudiziaria in materia penale nell'Unione europea al mandato europeo di ricerca delle prove e all'ordine europeo di indagine penale*, cit., p. 138; A. PERDUCA, *Prove, investigazioni e cooperazione giudiziaria su scala europea*, cit., p. 351; S. MONICI, *Emanate le norme di attuazione della Convenzione di assistenza giudiziaria in materia penale del 29 maggio 2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo d'indagine?*, in *eurojus.it*, 3 maggio 2017, disponibile al link: <http://rivista.eurojus.it/emanate-le-norme-di-attuazione-della-convenzione-di-assistenza-giudiziaria-in-materia-penale-del-29-maggio-2000-quali-margini-operativi-in-vista-dell'imminente-trasposizione-della-direttiva/?print=pdf>; A. NOCERA, *Le norme attuative della Convenzione*

accordi attualmente in vigore con Stati terzi, quali gli Stati Uniti ed il Giappone, nonché l'Islanda e il Regno di Norvegia, in materia di assistenza giudiziaria⁹³¹. Insufficiente – come si avrà modo di vedere – quanto previsto con la direttiva 2014/41/UE sull'ordine europeo di indagine.

Sebbene si tratti di strumenti che vanno nella direzione dell'incremento dell'efficienza e della rapidità della cooperazione tra Stati membri⁹³², tali fonti non contengono una disciplina specifica per questo particolare e delicato tipo di prova e, più in generale, per le indagini informatiche.

In tali casi, infatti, si ha bisogno di un approccio metodologico ed operativo parzialmente diverso in ragione delle caratteristiche strutturali dell'oggetto. È necessario, dunque, sviluppare sistemi che rispondano al principio di semplificazione e di rapidità nel processo di congelamento e assunzione di informazioni digitali detenute da prestatori di servizi stabiliti o rappresentati in un altro Stato membro⁹³³.

Pertanto, per verificare quanto sinora affermato, sarà necessario dapprima analizzare gli strumenti attualmente esistenti ed applicabili tra Stati membri dell'Unione europea, per poi procedere all'analisi delle proposte attualmente allo studio, al fine di individuare le criticità ed i punti di forza di quello che rappresenta il futuro della procedura penale europea.

europea di assistenza giudiziaria in materia penale (Bruxelles, 29 maggio 2000), in *ilpenalista.it*, 24 maggio 2017; J.P. PIERINI, *Assistenza giudiziaria a favore di autorità straniere e diritto di difesa: è vera incompatibilità?*, in *Cass. pen.*, 2, 2002, p. 1113 ss.; L. SALAZAR, *Genesi della Convenzione. La tardiva ratifica e la sua attuale operatività*, in AA.VV., *La nuova cooperazione giudiziaria penale. Dalle modifiche al Codice di Procedura Penale all'Ordine europeo di indagine penale* (a cura di M.R. MARCHETTI, E. SELVAGGI – coord. da G. BARROCU), Padova, 2019, p. 195 ss.; ID., *La nuova Convenzione europea sull'assistenza giudiziaria in materia penale* [I e II parte], in *Dir. pen. proc.*, 11, 2000, p. 1534 e 12, p. 1664; Z. SECCHI, *Le novità introdotte dalla Convenzione 9 maggio 2000 in tema di assistenza giudiziaria penale fra gli Stati membri dell'Unione europea*, in *Doc. giust.*, 6, 2000, p. 1108; F. TRAPPELLA, *Il provvedimento che attua la Convenzione di Bruxelles del 2000: una lunga gestazione e un destino incerto*, in *Proc. pen. e giust.*, 1, 2018, p. 17 ss.; N. TRIGGIANI, *In divenire la disciplina dei rapporti giurisdizionali con autorità straniere: appunti sulla l. 21 luglio 2016, n. 149*, cit., p. 1 ss.; O. VILLONI, G. DE AMICIS, *Il Protocollo della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea fatta a Bruxelles il 29 maggio 2000*, in *Cass. pen.*, 1, 2002, p. 421 ss.

⁹³¹ Il riferimento è all'Accordo sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, firmato il 25 giugno 2003, in GUUE L-181 del 19 luglio 2003, ed approvato a nome dell'Unione europea con Decisione 2009/820/PESC del 23 ottobre 2009, in GUUE L-291 del 7 novembre 2009, all'Accordo tra l'Unione europea e il Giappone relativo all'assistenza giudiziaria in materia penale firmato il 13 novembre 2009, in GUUE L-39 del 12 febbraio 2010, ed approvato a nome dell'Unione europea con Decisione 2010/616/UE del 7 ottobre 2010 in GUUE L-271 del 15 ottobre 2010, nonché all'Accordo tra l'Unione europea e la Repubblica d'Islanda e il Regno di Norvegia sull'applicazione di talune disposizioni della Convenzione del 29 maggio 2000 relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea e del relativo protocollo del 2001, firmato il 19 dicembre 2003, in GUUE L-26 del 29 gennaio 2004.

⁹³² Così, V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 441.

⁹³³ Sul punto, sia consentito il rinvio a A. GAUDIERI, *Opposizione al decreto di riconoscimento dell'ordine europeo di sequestro: scenari*, in *Giur. It.*, 8-9, 2020, p. 2033.

2. L'ordine europeo di indagine avente ad oggetto la prova elettronica

Un primo strumento all'avanguardia, basato sul principio del mutuo riconoscimento e ideato per la ricerca e formazione delle prove transnazionali tra Stati membri dell'Unione europea, è l'ordine europeo di indagine (OEI).

L'ordine europeo di indagine⁹³⁴, secondo l'art. 1 della direttiva 2014/41/UE⁹³⁵, è una decisione giudiziaria emessa o convalidata da un'autorità giudiziaria competente, rivolta

⁹³⁴ Secondo la dottrina, il termine “ordine d'indagine” sarebbe fuorviante relativamente alla sua effettiva funzione pratica da ricondurre non solo alle attività investigative in senso stretto ricomprese nella fase delle indagini preliminari, ma anche alle attività probatorie, svolte da un giudice nel processo penale. Infatti, si ritiene che il nome dato allo strumento sia doppiamente ingannevole e si tratterebbe di una imprecisione lessicale. Un primo aspetto ingannevole riguarderebbe la parola “indagine”. Questo perché il termine utilizzato rimanderebbe ad un'attività che, nel nostro sistema, si concretizza nella ricerca di elementi conoscitivi volti unicamente a stabilire se vi siano i presupposti per l'esercizio dell'azione penale, mentre le operazioni che possono esser compiute con un ordine europeo di indagine conducono all'assunzione di mezzi di prova, alla formazione di elementi di prova o addirittura all'acquisizione di vere e proprie prove. Tale imprecisione lessicale, però, svanisce del tutto nel corrispondente nome inglese (*European Investigation Order*), se si considera che il termine “*investigation*” ricomprende anche la ricerca delle prove. Dal punto di vista ontologico, vi sarebbe un secondo aspetto ingannevole: lo strumento più che a un ordine assomiglierebbe a una “richiesta” di adottare un determinato atto istruttorio da parte dell'autorità di emissione di uno Stato ed indirizzata ad uno Stato di esecuzione. Secondo lo schema classico dell'ordine così come ideato dal principio del mutuo riconoscimento, l'autorità di esecuzione sarebbe automaticamente tenuta ad attuare quanto indicato così come le viene rivolto; invece, con l'ordine europeo di indagine lo Stato di esecuzione ha la possibilità di impiegare modalità istruttorie diverse da quelle indicate, o addirittura di rifiutare l'esecuzione. Sul punto, M. DANIELE, *L'ordine europeo di indagine penale*, in *Atti del XXX Convegno Nazionale A.S.P.P. – Investigazioni e prove transnazionali*, Roma, 20-21 ottobre 2016, p. 1 ss., disponibile al sito web www.studiosiprocessopenale.it.

⁹³⁵ La Dir. 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, è pubblicata in G.U.U.E. L 130 del 1° maggio 2014. Tra i tanti commenti, S. ALLEGREZZA, *Collecting Criminal Evidence Across the European Union: the European Investigation Order Between Flexibility and Proportionality*, in AA.VV., *Transnational Evidence in Multicultural Inquiries* (a cura di S. RUGGERI), Heidelberg, 2014, p. 51 ss.; I. ARMADA, *The European Investigation Order and the Lack of European Standards for Gathering Evidence: is a Fundamental Rights-Based Refusal the Solution?*, cit., p. 8 ss.; L. BACHMAIER WINTER, *Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la orden europea de investigación*, in *Revista General de Derecho europeo*, 36, 2015, p. 15 ss.; ID., *Transnational evidence: towards the transposition of Directive 2014/41 regarding the European Investigation Order in criminal matters*, in *Eucrim: the European Criminal Law Associations'forum*, 2, 2015, p. 47 ss.; R. BELFIORE, *Riflessioni a margine della direttiva sull'Ordine europeo di indagine penale*, in *Cass. Pen.*, 9, 2015, p. 3288C ss.; J. BLACKSTOCK, *The European Investigation Order*, in *New Journal of European Criminal Law*, 4, 2010, p. 481 ss.; A. CABIALE, *Pubblicata la direttiva 2014/41/UE sull'ordine europeo d'indagine penale: semplificazioni, (s)fiducia reciproca e compromessi, per tentare di superare le rogatorie*, in *Proc. pen. e giust.*, 5, 2014, p. 15 ss.; M. CAIANIELLO, *L'OEI dalla direttiva al decreto n. 108 del 2017*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 17 ss.; ID., *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. pen. e giust.*, 3, 2015, p. 1 ss.; L. CAMALDO, *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *penalecontemporaneo.it*, 27 maggio 2014, p. 1 ss.; L. CAMALDO, F. CERQUA, *La direttiva sull'ordine europeo di indagine penale: le nuove prospettive per la libera circolazione delle prove*, in *Cass. Pen.*, 10, p. 3511 ss.; M. DANIELE, *Ordine europeo di indagine*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX Convegno nazionale A.S.P.P.*, Roma 20-21 ottobre 2016, Milano, 2017, p. 53 ss.; ID., *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, in *New Journal of European Criminal Law*, 6, 2015, p. 179 ss.; G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), cit., p. 991 ss.; G. DE AMICIS, *Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della*

direttamente ad un'autorità giudiziaria di un altro Stato membro per compiere uno o più atti di indagine specifici, al fine di acquisire degli elementi aventi attitudine probatoria⁹³⁶.

In effetti, si sostanzia in un provvedimento trasmesso direttamente dall'autorità di emissione a quella di esecuzione, da riconoscere ed eseguire in tempi rapidi, a meno che non vi siano circoscritti motivi di rifiuto o di rinvio che impediscano il compimento delle attività⁹³⁷.

cooperazione giudiziaria penale, in *Cass. pen.*, 1, 2018, p. 22 ss.; S. DEPAUW, *A European evidence (air)space? Taking cross-border legal admissibility of forensic evidence to a higher level*, in *European Criminal Law Review*, 1, 2016, p. 82 ss.; L. DOMÍNGUEZ RUIZ, *La orden europea de investigación: el camino hacia un régimen europeo uniforme en materia de prueba penal*, in AA.VV., *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales* (F. JIMÉNEZ CONDE, Director), Valencia, 2018, p. 337 ss.; A. IERMANO, *Sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera: l'ordine europeo di indagine penale (OEI)*, in *Diritto comunitario e degli scambi internazionali*, 3-4, 2015, p. 483 ss.; M. JIMENO BULNES, *Orden europea de investigación en materia penal*, in AA.VV., *Aproximación legislativa versus reconocimiento mutuo en el desarrollo del espacio judicial europeo: una perspectiva multidisciplinar* (M. JIMENO BULNES, Directora), Barcellona, 2016, p. 151 ss.; R. JURKA, *Movement of evidence in the European Union: Challenges for the European Investigation Order*, in *Baltic Journal of Law & Politics*, 2, 2016, p. 56 ss.; M.R. MARCHETTI, *Oltre le rogatorie: i nuovi strumenti per la circolazione degli atti investigativi e delle prove penali*, in AA.VV., *I nuovi orizzonti della giustizia penale europea. Atti del Convegno nazionale A.S.P.P.*, Milano, 24-26 ottobre 2014 (a cura di M.R. MARCHETTI), Milano, 2015, p. 207 ss.; R. PICCIRILLO, *I profili funzionali e strutturali dell'Ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 59 ss.; M. PISANI, *Problemi di prova in materia penale. La proposta di direttiva sull'Ordine Europeo di Indagine*, in *Arch. pen.*, 3, 2011, p. 14 ss.; F. SIRACUSANO, *The European Investigation Order for Evidence Gathering Abroad*, in *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office* (a cura di T. RAFARACI, R. BELFIORE), Cham, 2019, p. 85 ss.; ID., *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. Pen.*, 2, 2017, p. 1 ss.; A. TINOCO PASTRANA, *L'ordine europeo di indagine penale*, in *Proc. pen. e giust.*, 2, 2017, p. 346 ss.; T. RAFARACI, *General Considerations on the European Investigations Order*, in AA.VV., *Transnational Evidence and Multicultural Inquiries in Europe* (a cura di S. RUGGERI), Berlino, 2014, p. 37 ss.; C. RODRÍGUEZ-MEDEL NIETO, *Obtención y admisibilidad en España de la prueba penal transfronteriza. De las comisiones rogatorias a la orden europea de investigación*, Pamplona, 2016; M.^a I. ROMERO PRADAS, *La prueba penal en Europa, una cuestión compleja. La orden europea de investigación como nuevo instrumento de obtención de pruebas en procesos penales transnacionales y su próxima incorporación al Derecho español*, in AA.VV., *Integración europea y justicia penal* (M.^a I. GONZÁLEZ CANO, Directora), Valencia, 2018, p. 343 ss. Sull'applicazione dello strumento in caso di traffico di organi e di tratta di esseri umani v., L. KALB, S. NEGRI, *The Criminal Justice Response to Organ Trafficking and Trafficking in Human Beings for Organ Removal*, in *Journal of Trafficking and Human Exploitation*, 2, 2017, p. 187 ss.

⁹³⁶ Per un commento organico alla direttiva, si vedano i contributi in, T. BENE, L. LUPARIA, L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2016.

⁹³⁷ In tal senso, E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, in *Cass. pen.*, 3, 2020, p. 1303. Per uno studio sulla portata applicativa della direttiva, D. CIMADOMO, *Ordine europeo di indagine penale e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 219 ss.

Sebbene la direttiva abbia subito un *iter* abbastanza travagliato⁹³⁸, attualmente rappresenta l'esclusivo strumento⁹³⁹ per la formazione delle prove a carattere transfrontaliero tra gli Stati membri dell'Unione europea, avendo rimpiazzato i precedenti meccanismi farraginosi a carattere rogatorio⁹⁴⁰.

Invero, l'ordine europeo d'indagine ha consentito il superamento di un quadro normativo⁹⁴¹ in tema di formazione della prova particolarmente frammentario e

⁹³⁸ Il "Libro Verde sulla ricerca delle prove in materia penale tra Stati membri e sulla garanzia della loro ammissibilità" dell'11 novembre 2009 [COM(2009) 624 def.] prospettò per la prima volta la possibilità di introdurre uno strumento unico per la ricerca e la formazione transnazionale della prova, utilizzabile per qualsiasi tipologia di attività istruttoria, al fine di superare la frammentarietà e la disorganicità del quadro normativo esistente. Con il Programma di Stoccolma del 2009, si pianificò esplicitamente la creazione di un nuovo sistema unico e globale per la raccolta ed il trasferimento del dato probatorio basato sul principio del mutuo riconoscimento nell'Unione europea che sostituisse tutti gli strumenti già esistenti nel settore. Il "Programma Giustizia 2014-2020" ha prestato maggior attenzione anche ad altre forme di criminalità, quali il traffico di sostanze stupefacenti, considerando tra l'altro il rilevante impatto che determinano sull'economia. Inoltre, si dà grande importanza alla formazione dei giudici e dei professionisti al servizio dell'amministrazione della giustizia, facendo risaltare in tal modo temi che risultavano marginali nel Programma di Stoccolma. Tuttavia, non è stato semplice approvare la direttiva sull'ordine europeo di indagine. Infatti, la proposta di direttiva venne presentata al Consiglio nell'aprile 2010 da un gruppo di sette Stati membri, Austria, Belgio, Bulgaria, Estonia, Spagna, Slovenia e Svezia. L'accordo politico venne raggiunto nel dicembre 2011, ma alcune delegazioni nazionali preferirono mantenere una riserva parlamentare. Si avviarono, così, lunghe trattative, durate quattro anni, che portarono il 3 aprile 2014 alla direttiva 2014/41/UE. Sul tema, S. ALLEGREZZA, *Critical remarks on the Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9, 2010, p. 569 ss.; J.R. SPENCER, *The Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility: the Reaction of one British Lawyer*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9, 2010, p. 602 ss.

⁹³⁹ Cfr., A. GAITO, *Mandato di arresto europeo ed estradizione*, in AA.VV., *Procedura penale*, Torino, 2020, p. 1030, secondo il quale l'ordine europeo d'indagine rappresenta «l'unico strumento regolante l'acquisizione della prova nel territorio dell'Unione europea, implica il superamento dei previgenti strumenti giuridici».

⁹⁴⁰ Secondo A.A. DALIA, M. FERRAIOLI, *Manuale di diritto processuale penale*, cit., p. 1023, le rogatorie rappresentano una forma accessoria ed in ogni caso minore di collaborazione. Per uno studio relativo alla sostituzione delle "disposizioni corrispondenti" ad opera della direttiva 2014/41/UE, S. MONTALDO, *La scadenza del termine di recepimento della direttiva 2014/41/UE sull'ordine europeo di indagine penale e la sostituzione delle "disposizioni corrispondenti" della convenzione di assistenza giudiziaria tra gli Stati membri del 2000: spunti per la ricostruzione di un quadro normativo complesso*, in *Il diritto dell'Unione europea*, in *Il diritto dell'Unione europea*, 30 giugno 2017, p. 1 ss., disponibile al link: http://images.dirittounioneuropea.eu/f/sentenze/documento_D5ZJy_due.pdf.

⁹⁴¹ Secondo quanto previsto dall'art. 34 della direttiva 2014/41/UE, l'ordine europeo di indagine sostituisce la Convenzione di assistenza giudiziaria in materia penale del Consiglio d'Europa, del 20 aprile 1959 ed i protocolli aggiuntivi; la Convenzione di applicazione dell'accordo Schengen; la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea ed il relativo protocollo; la decisione quadro 2008/978/GAI in tema di mandato di ricerca della prova; la decisione quadro 2003/577/GAI relativa all'esecuzione dei provvedimenti di blocco dei beni e di sequestro probatorio. Tuttavia, tali atti non sono abrogati, ma continuano a rimanere in vigore per gli Stati che non hanno aderito alla direttiva, come Danimarca ed Irlanda. Inoltre, la Convenzione di Bruxelles del 2000 continua ad operare per tutti gli istituti non regolati dalla direttiva, come ad esempio le notificazioni o i rapporti con le autorità amministrative. Sul punto, G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), cit., p. 1002, secondo il quale la direttiva in materia di ordine europeo di indagine rappresenta un «punto di approdo di un percorso progettuale più ampio: di graduale sostituzione, nei rapporti tra Stati membri dell'UE, del tradizionale sistema di assistenza su base rogatoriale, regolamentato da norme di fonte internazionale pattizia, con un sistema integrato di ricerca e raccolta della prova basato su innovativi strumenti di carattere non rogatoriole, regolati dal diritto dell'Unione ed implicanti un rapporto diretto tra le autorità giudiziarie e di polizia, piuttosto che tra

disorganico⁹⁴², grazie all'attuazione della direttiva ed al successivo utilizzo dello strumento da parte di quasi la totalità degli Stati membri⁹⁴³.

governi». In merito all'art. 34 della direttiva 2014/41/UE, ci si è chiesti quale sia l'interpretazione corretta del termine "corrispondente". La corrispondenza formale prevede che la successione tra norme sia limitata «alle sole disposizioni le cui formulazioni siano identiche o che, quanto meno, presentino significative analogie»; mentre per la corrispondenza sostanziale «sarebbe invece sufficiente che le formulazioni interessate disciplinino in concreto lo stesso istituto, a prescindere dalla sovrapposibilità testuale». Tra "corrispondenza formale" e "corrispondenza sostanziale", la dottrina preferisce un approccio sostanziale, che trova un riscontro anche alla luce dell'interpretazione teleologica della formula, e risulta maggiormente in linea con la *ratio* della direttiva, volta alla semplificazione, velocizzazione e rafforzamento della cooperazione tra autorità giudiziarie nazionali in ambito probatorio. Questo perché la corrispondenza sostanziale si presta a una più ampia interpretazione che meglio si adegua ad una disciplina strettamente legata all'utilizzo di tecnologie in rapida evoluzione. Per un approfondimento, S. MONTALDO, *A caccia di... prove. L'ordine europeo di indagine penale tra complesse stratificazioni normative e recepimento nell'ordinamento italiano*, in *Giur. Pen.*, 11, 2017, p. 5.

⁹⁴² La dottrina ha evidenziato come lo strumento sia particolarmente moderno, perché coniuga il principio del mutuo riconoscimento e la flessibilità del sistema tradizionale basato sul principio della mutua assistenza giudiziaria. In tal senso, M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, cit., p. 90; S. RUGGERI, *Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issue*, in AA.VV., *Transnational Evidence and Multicultural Inquiries in Europe* (a cura di S. RUGGERI), Cham-Heidelberg-New York-Dordrecht-London, 2014, p. 9 ss.

⁹⁴³ La direttiva sull'ordine europeo di indagine è stata recepita da tutti gli Stati membri dell'Unione europea, ad eccezione di Danimarca ed Irlanda, nei confronti dei quali continueranno ad essere applicati i classici sistemi rogatori preesistenti. Il termine per il recepimento, ex art. 36 della stessa direttiva, è scaduto per gli Stati membri il 22 maggio 2017. A partire dal 1° gennaio 2021, nei rapporti tra Unione europea e Regno Unito si applicano la Convenzione europea di assistenza giudiziaria in materia penale, firmata a Strasburgo il 20 aprile 1959, il Protocollo addizionale alla Convenzione europea di assistenza giudiziaria, firmato a Strasburgo il 17 marzo 1978 ed il secondo Protocollo addizionale alla Convenzione europea di assistenza giudiziaria, firmato a Strasburgo l'8 novembre 2001, integrati dalle norme del titolo VIII dell'Accordo sugli scambi commerciali e la cooperazione tra l'Unione europea e la Comunità europea dell'energia atomica, da una parte, e il Regno Unito di Gran Bretagna e Irlanda del Nord, dall'altra, in G.U.U.E. L 444 del 31 dicembre 2020. In Italia, la direttiva è stata attuata con d.lgs. 21 giugno 2017, n. 108, contenente norme di attuazione della direttiva 2014/41/UE del Parlamento europeo e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale, pubblicato in G.U. 13 luglio 2017, n. 162, ed è entrato in vigore il 28 luglio 2017. Per un approfondimento, G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all'ordine europeo di indagine*, cit., p. 251 ss.; R. BELFIORE, *Su alcuni aspetti del decreto di attuazione dell'ordine europeo di indagine penale*, in *Cass. Pen.*, 1, 2018, p. 400 ss.; M. BOLOGNARI, *Ordine europeo di indagine penale ed esame a distanza*, in *Riv. dir. proc.*, 4-5, 2018, p. 1100 ss.; A. CABIALE, *I limiti alla prova nella procedura penale europea*, Milano, 2019, p. 249 ss.; M. CAIANIELLO, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. Pen.*, 6, 2018, p. 2197 ss.; L. CAMALDO, *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, in *Cass. Pen.*, 11, 2017, p. 4196B ss.; M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul D.Lgs. n. 108 del 2017*, in *Dir. Pen. Cont.*, 7-8, 2017, p. 208 ss.; G. DIOTALLEVI, *Dalle rogatorie all'ordine di indagine europeo*, in AA.VV., *lo spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. DI STASI, L.S. ROSSI), Napoli, 2020, p. 367 ss.; F. FALATO, *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale*, in *Arch. pen.*, 1, 2018, p. 1 ss.; E. GATTO, *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *dir. pen. cont.*, 2, 2019, p. 69 ss.; R.E. KOSTORIS, *Processo penale e paradigmi europei*, cit., 103 ss.; ID., *L'OEI nella dissolvenza tra regole e principi*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 3 ss.; ID., *Ordine di investigazione europeo e tutela dei diritti fondamentali*, in *Cass. pen.*, 5, 2018, p. 1437 ss.; E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, cit., p. 1302 ss.; A. MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa*

Ad oggi, la disciplina relativa all'ordine europeo di indagine è ritenuta la più avanzata⁹⁴⁴ in tema di ricerca e formazione della prova transnazionale mai adottata dal legislatore europeo, poiché tesa a rendere le attività di cooperazione più rapide, snelle ed agevoli⁹⁴⁵.

L'ordine europeo di indagine penale compie un passo avanti molto importante rispetto agli strumenti del passato perché costituisce un modello standardizzato di provvedimento investigativo/probatorio. Si tratta di uno strumento realistico, concreto, idoneo ad adattarsi all'attuale contesto dell'Unione europea, pensato soprattutto per essere utilizzato concretamente ed efficacemente⁹⁴⁶.

Caratteristica principale è l'onnicomprendività⁹⁴⁷. È uno strumento originale ma non del tutto innovativo. Infatti, mutua dalle classiche procedure una serie di caratteristiche ritenute efficienti, mentre per altri aspetti se ne distacca profondamente⁹⁴⁸.

all'ordine europeo di indagine penale, in *Dir. Pen. e Proc.*, 2, 2018, p. 158 ss.; M.R. MARCHETTI, *Ricerca e acquisizione probatoria all'estero: l'ordine europeo di indagine*, in *Arch. pen., speciale riforme*, 2018, p. 827 ss.; S. MARCOLINI, *L'ordine europeo di indagine alla prova dei fatti: prime pronunce in materia*, in *Cass. pen.*, 9, 2019, p. 3370 ss.; S. OPILIO, *L'ordine europeo di indagine penale*, in AA.VV., *Appunti di cooperazione giudiziaria penale* (a cura di F. FALATO), Napoli, 2019, p. 116 ss.; F. RUGGIERI, *Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale*, in *Proc. pen. e giust.*, 1, 2018, p. 12 ss.; E. SELVAGGI, *L'ordine europeo di indagine – EIO: come funziona?*, in *Cass. Pen.*, 1, 2018, p. 44B ss.; ID., *La circolare del Ministero della Giustizia sul c.d. ordine europeo di indagine*, in *Dir. pen. cont.*, 11, 2017, p. 287 ss.; P. SPAGNOLO, *I presupposti e i limiti dell'ordine di indagine europeo nella procedura passiva*, in AA.VV., *La nuova cooperazione giudiziaria penale* (a cura di M.R. MARCHETTI, E. SELVAGGI), Milano, 2019, p. 263 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 1110 ss.; M. TROGU, *Ordine europeo di indagine penale (d. lg. n. 108/2017)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 1004 ss. Per un confronto con l'ordinamento spagnolo v., A. TINOCO PASTRANA, *La transposición de la orden europea de investigación en materia penal en el ordenamiento español*, in *Rivista Freedom, Security & Justice: European Legal Studies*, 3, 2018, 116 ss.

⁹⁴⁴ La modernità ed il successo dello strumento sembrano confortati dai dati statistici. Alla maggior parte degli OEI è stata data esecuzione con esito positivo (tra il 76,65 % degli OEI cui è stata data esecuzione in uno Stato membro e il 96,93 % cui è stata data esecuzione in un altro Stato membro) e soltanto pochissimi OEI sono stati rifiutati (tra lo 0 % di tutti gli OEI emessi in uno Stato membro e il 17 % degli OEI emessi in un altro Stato membro). Tuttavia, in singoli casi – come per motivi di doppia incriminazione o perché non era possibile autorizzare un atto richiesto in conformità con il diritto interno, così come per ragioni di fatto o a causa di questioni di traduzione, compresi motivi quali la proporzionalità, le politiche de minimis e la pandemia di COVID-19, oltre a rifiuti senza motivazione – sono state registrate alcune questioni relative a rifiuti di dare esecuzione a OEI. Cfr., *Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della direttiva 2014/41/UE del Parlamento e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale*, Bruxelles, 20 luglio 2021, COM(2021) 409 final, p. 13.

⁹⁴⁵ In tal senso, S. ALLEGREZZA, A. MOSNA, F. NICOLICCHIA, *L'acquisizione della prova all'estero e i profili transnazionali*, in AA.VV., *Diritto penale delle società* (a cura di G. CANZIO, L.D. CERQUA, L. LUPARIA), Padova, 2016, p. 185 ss.; V. TONDI, *L'accesso transfrontaliero all'elettronic evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 443.

⁹⁴⁶ Di tale opinione è A. TINOCO PASTRANA, *L'ordine europeo di indagine penale*, cit., p. 358.

⁹⁴⁷ Sul carattere dell'“onnicomprendività” dell'Ordine europeo di indagine, si veda M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, cit., p. 3, il quale sottolinea che lo strumento è adottabile «per le prove reali e per quelle in senso lato documentali (così coprendosi l'area delle due decisioni quadro sul congelamento e la confisca dei beni, e sul mandato di ricerca delle prove); ancora, può essere emesso per acquisire una prova dichiarativa – da un potenziale testimone o da un imputato – così come per ottenere dati in tempo reale (ivi comprese le intercettazioni di comunicazioni). Infine, all'OEI si può ricorrere per effettuare un'operazione sotto copertura». Sugli effetti positivi dell'onnicomprendività e di uno strumento unico, si veda R. BELFIORE, *La prova penale “raccolta” all'estero*, cit., p. 208 ss.

⁹⁴⁸ È stato osservato che l'ordine europeo di indagine penale «non implica né l'unificazione né l'approssimazione delle legislazioni interne». Proprio in ciò lo strumento non appare innovativo, perché

L'onnicomprendività è uno degli elementi che determina l'efficienza dello strumento⁹⁴⁹. Essa è fondata su un corollario del principio del mutuo riconoscimento, ove determinante è ritenuta la flessibilità dei mezzi tesa, in funzione teleologica, al raggiungimento di un determinato risultato. Ovviamente, per fare ciò correttamente, è necessario compiere una valutazione di proporzionalità e legalità effettuata sia dall'autorità di emissione, sia dall'autorità di esecuzione⁹⁵⁰.

Infatti, l'ordine europeo è il frutto di una nuova impostazione che le istituzioni europee hanno voluto dare agli strumenti di cooperazione giudiziaria. Basandosi sull'art. 82, par. 1 TFUE, l'OEI intende proprio realizzare un «sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera», tale da sostituire «tutti gli strumenti esistenti nel settore» e da potersi utilizzare per «tutti i tipi di prove» stabilendo i termini di esecuzione e limitando al minimo i motivi di rifiuto⁹⁵¹. Per realizzare ciò, però, era necessario che l'OEI non fosse uno strumento di mutuo riconoscimento puro. Ed infatti, ne è scaturito uno strumento ibrido di cooperazione giudiziaria tra Stati membri dell'Unione europea che coniuga il principio del mutuo riconoscimento e la flessibilità del sistema tradizionale di mutua assistenza giudiziaria⁹⁵².

Lo strumento poggia le proprie basi operative sul principio di proporzionalità: vale a dire sulla tecnica ermeneutica volta a stabilire a quali condizioni ciascun principio possa

riproduce essenzialmente soluzioni che già esistono. Tuttavia, resta innegabile la sua maggior efficacia. Così, A. TINOCO PASTRANA, *L'ordine europeo di indagine penale*, cit., p. 350; F. MANFREDINI, *L'acquisizione probatoria in ambito europeo: i rapporti tra l'attività investigativa della procura europea e l'ordine europeo di indagine penale*, cit., p. 4227.; M. DANIELE, *L'ordine europeo di indagine penale*, cit., p. 1 ss.; R. DEL COCO, *Ordine europeo di indagine e poteri sanzionatori del giudice*, in *penalecontemporaneo.it*, 21 dicembre 2015, p. 6. Sugli elementi positivi che l'OEI ha mutuato dagli strumenti precedenti, R. BELFIORE, *La prova penale "raccolta" all'estero*, cit., p. 213 ss.; S. ALLEGREZZA, *Critical remarks on the Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility*, cit., p. 569 ss.; ID., *Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality*, in AA.VV., *Transnational Evidence and Multicultural Inquiries in Europe* (a cura di S. RUGGERI), cit., p. 53; M. PISANI, *Problemi di prova in materia penale. La proposta di direttiva sull'Ordine Europeo di Indagine*, cit., p. 5 ss.

⁹⁴⁹ L'OEI può esser usato per raccogliere un elemento probatorio durante tutte le fasi del procedimento penale, tendenzialmente per tutti i tipi di prove, sia precostituite che costituende, e non soltanto per l'esecuzione dell'atto investigativo o probatorio ma anche per il trasferimento del risultato. Una vera e propria innovazione se lo si confronta con i modelli precedentemente utilizzati.

⁹⁵⁰ In tal senso R. BELFIORE, *Riflessioni a margine della direttiva sull'ordine europeo di indagine penale*, cit., p. 3296.

⁹⁵¹ Si veda il considerando n. 5 e 6 della direttiva 2014/41/UE. Sul punto, anche, L. CAMALDO, *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, cit., p. 4196B ss.; M. DANIELE, *L'ordine europeo di indagine penale*, cit., p. 1 ss.; S. MONTALDO, *A caccia di... prove. L'ordine europeo di indagine penale tra complesse stratificazioni normative e recepimento nell'ordinamento italiano*, cit., p. 9 ss.

⁹⁵² In tal senso, M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, cit., p. 1 ss.; M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *penalecontemporaneo.it*, 20 novembre 2014, p. 3 ss.; E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurolunitario*, cit., p. 1303; F. SIRACUSANO, *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, cit., p. 1 ss.; ID., *La prova informatica transnazionale: un difficile «connubio» fra innovazione e tradizione*, cit., p. 187; A. TINOCO PASTRANA, *L'ordine europeo di indagine penale*, cit., p. 347. V. inoltre, G. UBERTIS, *Considerazioni generali su investigazioni e prove transnazionali*, in *Cass. pen.*, 1, 2017, p. 49B ss.

cedere di fronte all'esigenza di attuare valori contrapposti⁹⁵³. Dall'altra parte, esso assicura garanzie ineliminabili come la presunzione di innocenza ed i diritti di difesa, così come riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, anche attraverso quanto stabilito dall'art. 6 TUE, e dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali⁹⁵⁴.

⁹⁵³ Si tratta di una valutazione relativa al minor sacrificio. Il principio è, dunque, strumento di comparazione tra lo strumento utilizzato e la finalità dell'operazione, in ragione della gravità del reato per cui si procede. Sul principio di proporzionalità nell'OEI, M. DANIELE, *I chiaroscuri dell'OEI e la bussola della proporzionalità*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 55 ss.; E. GATTO, *Il principio di proporzionalità nell'ordine europeo di indagine penale*, cit., p. 69 ss. V., inoltre, S. ALLEGREZZA, *Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality*, cit., p. 59 ss.; I. ARMADA, *The European Investigation Order and the Lack of European Standards for Gathering Evidence: is a Fundamental Rights-Based Refusal the Solution?*, cit., p. 14 ss.; L. BACHMAIER WINTER, *The Role of the Proportionality Principle in Cross-Border Investigations Involving Fundamental Rights*, in AA.VV., *Transnational Inquiries ad the Protection of Fundamental Rights in Criminal Proceedings. A Study in Memory of Vittorio Grevi and Giovanni Tranchina* (a cura di S. RUGGERI), Berlino, 2013, p. 96 ss.; R. BELFIORE, *Riflessioni a margine della direttiva sull'ordine europeo di indagine penale*, cit., p. 3293; M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, cit., p. 145; F. FALATO, *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale*, cit., p. 1 ss.; D. HELENIUS, *Mutual Recognition in Criminal Matters and the Principle of Proportionality. Effective Proportionality or Proportionate Effectiveness?*, in *New Journal of European Criminal Law*, 3, 2014, p. 349 ss.; R.E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in AA.VV., *I nuovi orizzonti della giustizia penale europea. Atti del convegno. Milano, 24-26 ottobre 2014*, Milano, 2015, p. 56; G. UBERTIS, *Equità e proporzionalità versus legalità processuale: eterogenesi dei fini?*, in *Arch. pen.*, 2, 2017, p. 390 ss. Sul principio di proporzionalità, v. anche, T. A. ALEINIKOFF, *Constitutional Law in the Age of Balancing*, in *Yale Law Journal*, 96, 1987, p. 943 ss.; T.I. HARBO, *Introducing procedural proportionality review in European Law*, in *Leiden Journal of International Law*, 1, 2017, p. 25 ss.; E. HERLIN-KARNELL, *The domination of security and the promise of justice: on justification and proportionality in Europe's Area of Freedom, Security and Justice*, in *Transnational Legal Theory*, 1, 2017, p. 79 ss.; D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018* (a cura di L. KALB), cit., p. 55 ss.; G. PINO, *Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica*, 2, 2014, p. 541 ss.; G. SCACCIA, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle Corti europee*, in *Riv. AIC*, 3, 2017, p. 1 ss.; G. SILVESTRI, *L'individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018* (a cura di L. KALB), cit., p. 21 ss.; A. STONE SWEET, J. MATTHEWS, *Proportionality Balancing and Global Constitutionalism*, in *Columbia Journal of Transnational Law*, 47, 2008, p. 73 ss.; D. ŠUŠNJAR, *Proportionality, Fundamental Rights and Balance of Powers*, Leiden-Boston, 2010. In giurisprudenza, Cass., Sez. VI, sentenza del 25 febbraio 2019, n. 8320, in *Pluris*, secondo cui il principio di proporzionalità impone che l'attività da compiere debba essere adeguata e funzionale sia rispetto al suo presupposto (il reato), sia rispetto all'obiettivo che intende perseguire (le esigenze investigative o probatorie), in modo che la sua esecuzione comporti il minor sacrificio possibile per i diritti e le libertà dell'imputato o dell'indagato. Nello specifico, l'autorità giudiziaria deve valutare la capacità del mezzo richiesto di raggiungere l'obiettivo fissato, secondo il criterio per il quale, a parità di efficacia, è da preferire sempre il mezzo che abbia conseguenze meno gravose. La proporzionalità-adequatezza impone di porre in bilanciamento, da un lato, la restrizione imposta al singolo e, dall'altro, il valore del fine perseguito dal pubblico potere nell'esercizio della funzione. In questa valutazione, l'interprete sarà necessariamente guidato dalla natura del fatto per cui si procede.

⁹⁵⁴ Così, R.E. KOSTORIS, *L'OEI nella dissolvenza tra regole e principi*, cit., p. 7, secondo il quale il richiamo ai diritti fondamentali appare scontato, ma l'individuazione del contenuto di essi più difficile e certamente meno agevole, perché aventi un margine di indeterminatezza e variabilità. Infatti, i diritti tutelati dalla CEDU sono destinati a diventare il parametro di fondo anche delle tutele proprie dell'Unione europea, comprese quelle evocate nell'OEI. Tuttavia, se ciò «ha portato ad individuare un corposo ventaglio di

Sebbene si tratti di uno strumento basato sul principio del mutuo riconoscimento, non si è deciso di adottare un sistema “puro” caratterizzato dall’esclusiva applicazione della *lex fori*, bensì si è preferito recuperare i canoni della *lex loci*⁹⁵⁵, in coerenza con il più tradizionale metodo della mutua assistenza giudiziaria, allorché la *lex fori* non rispetti pienamente i principi fondamentali dello Stato di esecuzione⁹⁵⁶. Tale metodologia è volta a garantire il miglior accertamento dei fatti e l’efficienza processuale⁹⁵⁷.

Infatti, si sarebbe al cospetto di una combinazione virtuosa tra *lex loci* e *lex fori* che da un punto di vista teleologico è funzionale a raggiungere il risultato dell’utilizzabilità del dato probatorio nel Paese che ha richiesto l’OEI, con l’unico limite del rispetto dei principi fondamentali dell’ordinamento dello Stato di esecuzione nel compimento degli atti o delle formalità.

Dal punto di vista sistematico, come di consueto quando si tratta di strumenti di assistenza giudiziaria internazionale, si distingue la procedura passiva⁹⁵⁸ – o richiesta dall’estero – in Italia disciplinata dagli artt. 4 e ss., d.lgs. 21 giugno 2017, n. 108, raggruppati nel titolo II, dalla procedura attiva – o richiesta all’estero – le cui regole sono previste nel titolo III, agli artt. 27 e ss., d.lgs. 21 giugno 2021, n. 108.

Per quanto attiene alle fasi del procedimento, a chi ritiene che gli snodi del procedimento probatorio mediante uso dell’ordine europeo d’indagine siano quattro (emissione, riconoscimento, esecuzione ed impugnazione)⁹⁵⁹, si affianca chi individua solo tre momenti essenziali (ammissione degli atti istruttori indicati nell’OEI, la raccolta e l’utilizzazione delle prove)⁹⁶⁰.

specificazioni di tali diritti, soprattutto sul versante dell’equità processuale, ne ha reso, per così dire, anche meno “stabili” i contenuti. Ciò è dovuto al limite intrinseco che deriva dalla stessa fisionomia della Corte europea, la quale cumula in sé la doppia veste di organo nomofilattico e di giudice dei casi concreti; ruolo quest’ultimo che la porta a parametrare le sue decisioni sulle peculiari caratteristiche della vicenda giudiziaria sottoposta al suo vaglio, potendo giungere a soluzioni diverse per casi astrattamente simili, ma caratterizzati da componenti fattuali diverse, con conseguenti possibili mutamenti di interpretazione delle medesime garanzie, che però sono destinati a creare disorientamento nel momento in cui il *case law* di Strasburgo diventa un parametro generale di riferimento per l’individuazione dei diritti fondamentali anche rispetto al diritto dell’Unione». Sul punto, anche, E. LORENZETTO, *L’ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, cit., p. 1303.

⁹⁵⁵ La dottrina parla di forma ibrida tra *lex loci* e *lex fori*. In tal senso, L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, in AA.VV., *L’ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), cit., p. 22.

⁹⁵⁶ In tal senso, E. LORENZETTO, *L’ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, cit., p. 1303; E. SELVAGGI, *La circolare del Ministero della giustizia sul c.d. Ordine Europeo di Indagine*, cit., p. 1 ss.; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, in *New Journal of European Criminal Law*, 2, 2020, p. 164.

⁹⁵⁷ Cfr., M. DANIELE, *La metamorfosi del diritto delle prove nella Direttiva sull’ordine europeo di indagine penale*, cit., p. 3 ss.; A. TINOCO PASTRANA, *L’ordine europeo di indagine penale*, cit., p. 347.

⁹⁵⁸ Sulla prassi operativa per gli ordini europei passivi, v. la circolare della Procura della Repubblica presso il Tribunale di Torino *Principi interpretativi e prassi operative per OEI passivi*, in *Sistema Penale*, recuperabile al seguente link: https://www.sistemapenale.it/pdf_contenuti/1612720796_procura-di-torino-2021-circolare-ordine-europeo-indagine-oei-passivo.pdf. Per alcune interessanti riflessioni sulla procedura passiva, G. MAZZA, *Ordine europeo di indagine: la forma soccombe davanti alla sostanziale assenza di pregiudizio*, in *dir. pen. e proc.*, 10, 2021, p. 1343 ss.

⁹⁵⁹ Così, E. LORENZETTO, *L’ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, cit., p. 1304.

⁹⁶⁰ Cfr., M. DANIELE, *Ordine europeo di indagine*, in AA.VV., *Investigazioni e prove transnazionali*, cit., p. 54.

Accanto a questi due meritevoli orientamenti, potrebbe proporsi una diversa divisione in fasi, frutto di una riflessione partita proprio dalle due posizioni appena descritte. Da una lettura sistematica della direttiva 2014/41/UE e del d.lgs. 21 giugno 2017, n. 108, sembrerebbe opportuno individuare quattro fasi del procedimento: emissione, riconoscimento, esecuzione e trasferimento della prova. Accanto a queste si porrebbe la fase eventuale ed incidentale dell'impugnazione.

Da qui sembra opportuno partire per verificare se lo strumento dell'OEI risulta idoneo ed efficiente per la ricerca e formazione di elementi digitali aventi attitudine probatoria.

Dunque, è necessario descrivere brevemente le varie fasi del procedimento per individuare gli eventuali momenti di frizione rispetto alle caratteristiche proprie della c.d. prova informatica.

Preliminarmente, va chiarito che sebbene possa essere utilizzato per «tutti gli atti di indagine finalizzati all'acquisizione della prova»⁹⁶¹, la direttiva non individua una specifica disciplina per questo particolare tipo di elemento avente attitudine probatoria, come invece avviene per altre attività o altri atti d'indagine⁹⁶².

Parimenti, nei testi normativi non si fa alcun riferimento diretto a prove a carattere digitale. Tuttavia, sia la direttiva sia il decreto legislativo di recepimento farebbero cenno esclusivamente alle informazioni relative all'abbonato.

Invero, l'art. 10, par. 2, lett. e) della direttiva 2014/41/UE dispone che deve sempre essere disponibile in base al diritto dello Stato membro di esecuzione l'individuazione di persone titolari di un abbonamento a uno specifico indirizzo IP. Di conseguenza, l'art. 9, comma 5, d.lgs. 21 giugno 2017, n. 108 dispone che sia dato in ogni caso esecuzione all'ordine europeo di indagine avente ad oggetto l'identificazione di persone titolari di un indirizzo di posta elettronica o di un indirizzo IP.

Orbene, appare pacifico che, nonostante ciò, le autorità giudiziarie debbano eseguire attività investigativo-probatorie applicando la disciplina relativa alle ispezioni, le perquisizioni ed ai sequestri informatici, nel rispetto dei protocolli tecnici indispensabili per garantire l'affidabilità e la genuinità del dato digitale⁹⁶³.

Parimenti, per le intercettazioni⁹⁶⁴ (la cui disciplina è sistematicamente articolata in quattro ipotesi: attiva e passiva, con o senza la necessità di assistenza tecnica), per quanto

⁹⁶¹ Cfr., *considerando* n. 8, direttiva 2014/41/UE.

⁹⁶² Il riferimento è al trasferimento temporaneo delle persone detenute ai fini di un atto d'indagine, all'audizione mediante videoconferenza o altra trasmissione audiovisiva, all'audizione mediante teleconferenza, alle informazioni relative a conti bancari e altri conti finanziari, alle informazioni relative a operazioni bancarie e ad altre operazioni finanziarie, agli atti di indagine che implicano l'acquisizione di elementi di prova in tempo reale, in modo continuo e per un periodo determinato, alle operazioni sotto copertura, alle intercettazioni, ai provvedimenti provvisori, disciplinati ai Capi IV, V e VI della direttiva 2014/41/UE. Per quanto attiene, invece, a quanto stabilito con la disciplina interna di recepimento della direttiva, con il d.lgs. 21 giugno 2017, n. 108 è stata individuata una disciplina specifica per: il trasferimento temporaneo di persone detenute (artt. 16, 17, 37 e 38); l'audizione mediante videoconferenza o altra trasmissione audiovisiva (artt. 18 e 39); l'audizione mediante teleconferenza (art. 19); le informazioni e i documenti presso banche e istituti finanziari (artt. 20 e 40); le operazioni sotto copertura (artt. 21 e 41), le intercettazioni (artt. 23, 24, 25, 43, 44, 45); il sequestro (art. 26).

⁹⁶³ In tal senso, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in AA.VV., *Cybercrime* (a cura di A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), cit., p. 1623.

⁹⁶⁴ Per un approfondimento sull'ordine europeo di intercettazione, più ampiamente, L. GIORDANO, *La direttiva OEI e la disciplina delle intercettazioni "transfrontaliere": è alla fine la stagione dell'instradamento?*, in *La Magistratura*, 3, 2017, p. 93 ss.; ID., *Intercettazioni: è al tramonto la stagione dell'instradamento?*, in *ilpenalista.it*, 12 giugno 2017, disponibile al seguente link: <https://ilpenalista.it/articoli/focus/intercettazioni-al-tramonto-la-stagione-dellinstradamento>; A. NOCERA,

attiene alla procedura passiva, l'art. 24 del d.lgs. 21 giugno 2017, n. 108 consente l'intercettazione con la tecnica dell'instradamento⁹⁶⁵ anche di un sistema informatico o telematico in uso alla persona che si trovi nel territorio dello Stato.

In tali casi, il Procuratore della Repubblica ha un onere formale di trasmissione, dovendo inviare immediatamente al giudice per le indagini preliminari la notificazione dell'avvio delle operazioni effettuata dall'autorità giudiziaria dello Stato membro che procede. A questo punto, se le intercettazioni sono state disposte in riferimento a un reato per il quale, secondo l'ordinamento interno, le captazioni non sono consentite, il giudice per le indagini preliminari ordina l'immediata cessazione delle operazioni e contestualmente lo comunica al Procuratore della Repubblica, il quale, senza ritardo, e non oltre novantasei ore dalla ricezione della notifica, dà comunicazione all'autorità giudiziaria dello Stato di emissione del provvedimento di cessazione delle operazioni e della non utilizzabilità ai fini della prova dei risultati delle intercettazioni eseguite.

Si tratta di ipotesi definite "semplificate" o "leggere" per il quale è previsto un mero obbligo di notifica allo Stato nel quale si trovi l'utenza, l'apparecchio mobile o il soggetto da captare. Non è previsto nessun controllo di ammissibilità da parte del Procuratore della

Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione, in *dir. pen. cont.*, 1, 2018, p. 149 ss.; C. PARODI, *Ordine europeo di indagine: la disciplina delle intercettazioni*, in *Cass. pen.*, 3, 2020, p. 1314 ss.; ID., *Il recepimento della direttiva 2014/41/UE: le disposizioni in tema di intercettazioni*, in *studiosiprocessopenale.it*, p. 1 ss., disponibile al seguente link: <http://www.studiosiprocessopenale.it/download/XchOulJ-ulkkROcmc1Lqz0UGX4r9UrNA0w1MaRxcAsE/c-parodi-disposizioni-in-tema-di-intercettazioni.pdf>.

⁹⁶⁵ La tecnica dell'instradamento è un metodo di intercettazione che non necessita dell'assistenza dell'autorità giudiziaria dello Stato di esecuzione perché avviene attraverso la canalizzazione dei flussi comunicativi su impianti e ripetitori ubicati nel territorio dello Stato di emissione. Su tale metodologia, *ex multis*, E. APRILE, *Nuovi strumenti e tecniche investigative nell'ambito U.E.: intercettazioni all'estero, operazioni di polizia oltre frontiera, attività sotto copertura e videoconferenze con l'estero*, in *Cass. pen.*, 1, 2009, p. 440B ss.; A. BALSAMO, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in *Cass. pen.*, 11, 2016, p. 4236 ss.; A. BARGI, *Intercettazioni telefoniche: effettività della difesa e imprevedibilità delle decisioni di legittimità*, in *Giur. It.*, 3, 2011, p. 729 ss.; T. BENE, *Transnazionalità dei crimini nella società confessionale: i pericoli della tecnologia e del diritto*, in *Giur. It.*, 3, 2016, p. 717 ss.; V. CAMPILONGO, *L'obbligo di motivazione in tema di intercettazioni di conversazioni o comunicazioni: questioni interpretative e problemi applicativi*, in *Cass. pen.*, 10, 2005, p. 3196 ss.; C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, 10, 2011, p. 3638B; A. DIDI, *Il regime delle intercettazioni telefoniche per «instradamento»*, in *Giust. pen.*, 3, 2001, p. 126 ss.; L. GIORDANO, *Captatore informatico: utilizzabili anche le conversazioni intercettate all'estero*, in *ilprocessotelematico.it*, 18 dicembre 2020; ID., *L'intercettazione delle e-mail (già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze"*, in *ilpenalista.it*, 14 novembre 2016; E.N. LA ROCCA, *Intercettazioni, utilizzo di impianti esterni, instradamento: garanzie tecniche e prassi devianti*, in *Giur. It.*, 3, 2011, p. 731 ss.; W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, cit., p. 278 ss.; L. PISTORELLI, *Le Sezioni Unite di fronte alle sfide della modernità: le pratiche di "remotizzazione" delle intercettazioni*, in *Cass. pen.*, 1, 2009, p. 40 ss.; F. RUGGIERI, *Le intercettazioni «per instradamento» sul canale internazionale: un mezzo di ricerca della prova illegittimo*, in *Cass. pen.*, 4, 2000, p. 1058 ss.; M. TIBERI, *L'instradamento delle telefonate straniere: una prassi discutibile*, in *Cass. pen.*, 3, 2004, p. 959 ss.; A. UBALDI, *Intercettazioni ambientali all'estero: microspia in auto senza rogatoria*, in *Dir. & giustizia*, 131, 2018, p. 8 ss.

Repubblica, il quale funge solo da mero organo di trasmissione della notificazione⁹⁶⁶, e la captazione avviene direttamente da parte dello Stato di emissione in base alla *lex fori*⁹⁶⁷.

Quando, invece, lo Stato di esecuzione riceve un ordine europeo d'indagine per l'acquisizione di dati relativi alle comunicazioni telematiche, ai sensi dell'art. 25, d.lgs. 21 giugno 2017, n. 108, il Procuratore della Repubblica legittimato ne dà esecuzione con le forme e le modalità previste dall'art. 256 c.p.p.

Infine, nell'ambito degli atti d'indagine richiesti dall'estero, l'art. 20, comma 2, del d.lgs. 21 giugno 2017, n. 108 consente l'acquisizione "dinamica" – e, dunque, in tempo reale – dei flussi informatici o telematici provenienti o diretti a banche e istituti finanziari relativi ai conti, prevedendo che il Procuratore della Repubblica provveda, se necessario, mediante richiesta al giudice per le indagini preliminari, secondo quanto previsto dagli artt. 266 e ss. c.p.p.

Per quanto attiene alla procedura attiva, l'art. 43, d.lgs. 21 giugno 2017, n. 108, disciplina l'ordine di intercettazione con assistenza tecnica dell'autorità giudiziaria di un altro Stato membro. Si tratta dei casi in cui l'autorità giudiziaria italiana deve intercettare comunicazioni o conversazioni estero su estero, non dirottabili su nodi telefonici ubicati in Italia e per cui è necessario richiedere assistenza tecnica.

In tali ipotesi, la normativa consente all'ufficio del pubblico ministero – autorizzato dal giudice per le indagini preliminari a svolgere un'attività captativa – di emettere, mediante la trasmissione allo Stato di esecuzione di un modulo *standard*, un ordine di indagine con il quale si richiede l'assistenza tecnica all'esecuzione delle operazioni d'intercettazione non solo delle conversazioni o comunicazioni, ma anche del flusso di comunicazioni relativo a sistemi informatici o telematici.

Inoltre, ai sensi dell'art. 45, d.lgs. 21 giugno 2017, n. 108, «il pubblico ministero o il giudice che procede possono trasmettere all'autorità di esecuzione ordine di indagine al fine di ottenere i dati esterni relativi al traffico [...] telematico nonché l'acquisizione di ogni altra informazione utile in possesso degli operatori di telecomunicazioni»⁹⁶⁸.

Ai sensi dell'art. 28 della direttiva 2014/41/UE, l'acquisizione può avvenire per un tempo determinato e l'autorità di emissione deve indicare le ragioni per le quali le informazioni richieste assumano il carattere dell'utilità per il procedimento penale nazionale. Ai fini del riconoscimento, essendo un atto coercitivo, va valutato secondo proporzionalità e tenendo conto degli altri motivi di rifiuto previsti per le altre attività⁹⁶⁹.

La disciplina di settore, tuttavia, si limita a queste disposizioni relative all'acquisizione di dati informatici o telematici in tempo reale, lasciando che per le altre attività si utilizzi una procedura evidentemente poco idonea e funzionale a raggiungere lo scopo, in ragione delle particolari caratteristiche della prova informatica.

Sul versante delle disposizioni generali la situazione non sembra migliorare, complice una disciplina che prevede una tempistica lenta e farraginosa rispetto alla velocità con cui

⁹⁶⁶ Dunque, non è prevista nessuna particolare formalità da rispettare se non la semplice verifica da parte del giudice per le indagini preliminari che si tratti di una intercettazione disposta in riferimento a un reato per il quale sono consentite le intercettazioni secondo l'ordinamento interno. Cfr. A. NOCERA, *Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione*, cit., p. 153.

⁹⁶⁷ Così, M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, cit., p. 1636.

⁹⁶⁸ Il modulo dovrà riportare i dati tecnici necessari all'individuazione del sistema informatico, ogni informazione utile ai fini dell'identificazione della persona che li ha in uso e dell'operatore, se noti, nonché l'indicazione del reato per il quale si procede.

⁹⁶⁹ In tal senso, F. SIRACUSANO, *La prova informatica transnazionale: un difficile "connubio" fra innovazione e tradizione*, cit., p. 188.

circolano e si dissolvono i dati elettronici⁹⁷⁰. Alle gambe possenti su cui corrono gli elementi digitali, si contrappongono le brachicardiche attività tradizionali con cui si raccolgono i dati informatici, al cui naturale decorso del tempo necessario per l'attività investigativo-probatoria propriamente intesa, si aggiungono i tempi non di certo brevi – in relazione a queste specifiche tipologie di attività – delle fasi proprie del procedimento relativo all'ordine europeo di indagine.

Volendo descrivere brevemente la disciplina, il procedimento si attiva con l'emissione dell'ordine da parte dell'autorità di uno Stato membro⁹⁷¹. Tale autorità⁹⁷², ai sensi dell'art. 6 della direttiva 2014/41/UE, deve verificare la necessità e la proporzionalità (ai fini del procedimento in questione) e che l'OEI avrebbe potuto essere emesso alle stesse condizioni in un caso interno analogo⁹⁷³.

La trasmissione del modulo *standard*, correttamente compilato e debitamente tradotto, avviene – secondo quanto stabilito dall'art. 7 della direttiva 2014/41/UE⁹⁷⁴ – direttamente

⁹⁷⁰ Sul punto, F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, in *magistraturaindipendente.it*, 6 giugno 2019, disponibile al link: <https://www.magistraturaindipendente.it/lordine-di-produzione-e-di-conservazione-europeo-delle-prove-elettroniche.htm>, secondo la quale «l'ordine di indagine europeo (O.E.I.) si rivela da un lato troppo lento rispetto alle urgenti esigenze punitive avanzate a fronte di reati caratterizzati da elevato allarme sociale quali quelli concernenti il terrorismo e più in generale il crimine transnazionale, dall'altro si rivela infruttuoso, se solo si tenga a mente come molte delle società che gestiscono i dati abbiano sede in alcuni Stati (come l'Irlanda) che non hanno aderito ad importanti strumenti legislativi quali la direttiva che ha introdotto l'O.E.I.».

⁹⁷¹ In Italia, ai sensi dell'art. 27, d.lgs. 21 giugno 2017, n. 108, l'ufficio del pubblico ministero e il giudice, nell'ambito delle rispettive attribuzioni. L'ordine non può essere direttamente emesso da un difensore della persona sottoposta alle indagini, dell'imputato, della persona per la quale è proposta l'applicazione di una misura di prevenzione. Tuttavia, in ossequio a quanto disposto dall'art. 31, d.lgs. 21 giugno 2017, n. 108, il difensore di questi può chiedere all'ufficio del pubblico ministero o al giudice che procede l'emissione di un ordine. Si tratta dunque, solo di un potere di compulsione dell'organo legittimato, poiché la richiesta deve avvenire secondo la tecnica della “canalizzazione” della richiesta, ossia di “mediazione”, particolarmente criticata in dottrina. Inoltre, la norma lascerebbe privi di qualsiasi strumento utile gli altri difensori, tra cui soprattutto quello della persona offesa. Sul punto, D. CIMADOMO, *Ordine europeo di indagine e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, cit., p. 224. V., anche, M. CAGOSI, *Un illustre assente: la vittima del reato nell'ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 119 ss. In una logica aperturista, basata sulla considerazione che la cooperazione giudiziaria resta in ogni caso una prerogativa degli Stati, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 89 ss.

⁹⁷² L'art. 2, par. 1, lett. c) della direttiva 2014/41/UE indica – quali autorità di emissione – un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato o qualsiasi altra autorità competente che nel caso di specie agisca in qualità di autorità inquirente nel processo penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale. Sulle caratteristiche dell'autorità emittente l'ordine europeo di indagine penale, S. QUATTROCOLO, *Nozioni autonome o variabili? La Corte di giustizia e la definizione di «autorità giudiziaria» e «autorità emittente» nel sistema della cooperazione giudiziaria infraeuropea. Riflessioni a margine di due recenti pronunce*, in *Cass. pen.*, 5, 2021, p. 1792 ss. Sullo stesso tema, volendo, A. GAUDIERI, *Conformità del rapporto di subordinazione del pubblico ministero con la direttiva 2014/41/UE: l'orientamento adottato dalla Corte di giustizia nella sentenza A. e A.*, in *slog.unisa.it*, dicembre 2020, p. 1 ss., disponibile al link: <https://www.unisa.it/uploads/14394/audieri.dic.2020.nota.pdf>.

⁹⁷³ Secondo la dottrina, tali condizioni rappresenterebbero una barriera al *forum shopping*. In tal senso, K. AMBOS, *European Criminal Law*, Cambridge, 2018, p. 458 ss.; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 165.

⁹⁷⁴ Per la disciplina interna, v., l'art. 27, d.lgs. 21 giugno 2017, n. 108.

all'autorità dello Stato membro di esecuzione, così come dirette sono anche le successive comunicazioni, in modo da lasciarne traccia e da stabilirne l'autenticità. La promozione del dialogo è così forte che le autorità possono concordare le modalità del compimento dell'attività ad oggetto dell'ordine, tenendo conto delle regole nazionali, dei diritti e delle facoltà che la legge accorda alle parti.

In funzione della natura, della complessità e dell'urgenza del caso, per accelerare la trasmissione degli OEI e garantire l'autenticità si utilizzano canali differenti, tra cui Eurojust, i punti di contatto della RGE e i magistrati di collegamento. Inoltre, è in fase di sviluppo da parte dell'Unione europea un portale *online* protetto, che funga da rete di comunicazione e trasmissione dei modelli: l'*e-CODEX (e-Justice Communication through On-line Data Exchange)*⁹⁷⁵.

La Commissione ha, altresì, sviluppato il sistema digitale di scambio di prove elettroniche (*e-Evidence Digital Exchange System*, eEDES), uno strumento informatico che gli Stati membri possono utilizzare per scambiarsi in modo rapido e sicuro ordini europei di indagine in formato digitale in conformità con le prescrizioni stabilite nella direttiva. Il sistema può, inoltre, essere utilizzato per trasmettere le prove elettroniche e le prove associate dallo Stato membro di esecuzione a quello di emissione⁹⁷⁶. La Commissione ha incoraggiato tutti gli Stati membri a connettersi all'eEDES, in quanto si prevede che ciò aumenterà ulteriormente l'efficienza della direttiva 2014/41/UE⁹⁷⁷.

Una volta ricevuto l'ordine, l'autorità giudiziaria procede al riconoscimento dell'ordine europeo di indagine⁹⁷⁸, se non sussistano motivi di rifiuto e di restituzione di cui all'art. 11 della direttiva 2014/41/UE⁹⁷⁹, tra cui immunità o privilegi, ovvero norme

⁹⁷⁵ L'*e-CODEX* è un sistema informatico decentralizzato per le comunicazioni transfrontaliere che faciliterà la trasmissione di documenti, richieste, formulari giuridici, prove o altre informazioni in modo sicuro e affidabile, tanto per i procedimenti penali, quanto per i procedimenti civili a carattere transfrontaliero. *E-CODEX* è stato lanciato nell'ambito del piano d'azione pluriennale 2009-2013 in materia di giustizia elettronica, con lo scopo principale di promuovere la digitalizzazione dei procedimenti giudiziari transfrontalieri e facilitare la comunicazione tra le autorità giudiziarie degli Stati membri. Si tratta di un pacchetto *software* che può essere utilizzato per istituire un punto di accesso per una comunicazione sicura. I punti di accesso possono comunicare tra loro via internet attraverso una serie comune di protocolli, senza l'intervento di un sistema centrale. Il sistema è stato messo a punto da 21 Stati membri – tra cui l'Italia – con la partecipazione di altri Paesi e organizzazioni terzi tra il 2010 e il 2016. Attualmente, il sistema *e-CODEX* è già operativo in alcuni Stati membri che sono i promotori iniziali di questo progetto ed in futuro potrebbe diventare la soluzione digitale primaria per una trasmissione sicura di dati elettronici nei processi civili e penali transfrontalieri nell'Unione. Il Comitato economico e sociale europeo si spinge sino a ritenere che dovrebbero essere resi possibili anche altri impieghi da parte di altre amministrazioni pubbliche, tra cui, ad esempio, il trasferimento del fascicolo sanitario elettronico. Anche il portale europeo della giustizia elettronica si servirà del sistema, mentre l'impiego nel settore penale renderà la cooperazione giudiziaria in materia penale più efficiente, intensificando in tal modo la lotta alla criminalità transfrontaliera, al terrorismo e alla criminalità informatica. Cfr., *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un sistema informatizzato di comunicazione per i procedimenti civili e penali transfrontalieri (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726*, 2.12.2020, [COM/2020/712 final].

⁹⁷⁶ Giova qui ricordare che eEDES utilizza già eCODEX. Cfr., *Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della direttiva 2014/41/UE del Parlamento e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale*, Bruxelles, 20 luglio 2021, COM(2021) 409 final, p. 16 ss.;

⁹⁷⁷ Così, Comunicazione della Commissione al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, *"Digitalizzazione della giustizia nell'Unione europea – Un pacchetto di opportunità*, Bruxelles, 2 dicembre 2020, p. 18 ss.

⁹⁷⁸ Sul riconoscimento dell'OEI, A. FABBRICATORE, *Effetti della ritardata comunicazione del decreto di riconoscimento dell'OEI*, in *Giur. It.*, 6, 2021, p. 1476 ss.

⁹⁷⁹ Per la disciplina interna, cfr., art. 10, d.lgs., 21 giugno 2017, n. 108.

di determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione che renderebbero impossibile l'esecuzione dell'OEI; casi specifici che possano ledere interessi di sicurezza nazionale o che possano mettere in pericolo la fonte delle informazioni o che comportino l'uso di informazioni o segreti relativi alle attività di *intelligence*; *ne bis in idem*; questioni relative alla territorialità o alla tutela dei diritti fondamentali⁹⁸⁰; assenza della doppia incriminazione⁹⁸¹; uso limitato o non disponibile per il reato richiesto nello Stato di esecuzione⁹⁸².

Tuttavia, in talune ipotesi, prima di non riconoscere il provvedimento, l'autorità può avviare un dialogo, finalizzato ad ottenere nuove informazioni utili per l'eventuale riconoscimento e qualora sussista un atto di indagine alternativo nel proprio Stato, può disporre questo⁹⁸³.

Il riconoscimento dell'ordine rappresenta una fase autonoma rispetto a quella di esecuzione, in cui vi è un controllo penetrante relativo al rispetto delle condizioni richieste⁹⁸⁴. Questa fase si sostanzia per essere un momento di valutazione, comunicazione e confronto, in relazione alle attività da svolgere. Infatti, il decreto di riconoscimento dell'ordine, generalmente, va comunicato al difensore della persona sottoposta alle indagini⁹⁸⁵.

⁹⁸⁰ Sullo specifico motivo di rifiuto relativo alla tutela dei diritti fondamentali, P. SPAGNOLO, *La nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, cit., p. 1290 ss.

⁹⁸¹ Tuttavia, tale motivo di rifiuto non opera per i reati individuati all'art. 11, d.lgs. 21 giugno 2017, n. 108. Sul criterio della doppia incriminazione, F. MAZZACUVA, *La doppia incriminazione e la deroga per i reati di "lista positiva"*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 136 ss.; M. TROGU, sub art. 11, *Ordine europeo di indagine penale*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), cit., p. 1043 ss.

⁹⁸² Sul controllo relativo al contenuto dell'ordine europeo di indagine penale, R. BELFIORE, *La prova penale "raccolta" all'estero*, cit., p. 225 ss.; L. CAMALDO, *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, cit., p. 4196 ss.; M. DANIELE, *Ricerca e formazione della prova – Profili generali*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 470 ss.; G. FIORELLI, *I motivi di rifiuto dell'ordine investigativo europeo, quando "fidarsi è bene, ma non fidarsi è meglio"*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 84 ss.; A. MANGIARACINA, *Il procedimento di esecuzione dell'OEI e i margini nazionali di rifiuto*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 118 ss.; A. TINOCO PASTRANA, *L'ordine europeo di indagine penale*, cit., p. 355; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 166.

⁹⁸³ Cfr., artt. 10 e 11, della direttiva 2014/41/UE, nonché, artt. 6 e 9, d.lgs. 21 giugno 2017, n. 108.

⁹⁸⁴ Così, E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, cit., 1306.

⁹⁸⁵ La dottrina ha osservato come la disciplina non fornisca indicazioni precise su quale sia il difensore a cui vada comunicato il decreto di riconoscimento. Sembra, perciò, riferirsi al difensore straniero che già assiste la persona sottoposta alle indagini nel procedimento di cognizione principale. Dunque, sembrerebbe sussistere la necessità di nominare o designare d'ufficio un difensore italiano, in sostegno alle attività del difensore straniero. Va ricordato che l'esercizio della professione forense in Italia per coloro i quali sono abilitati in un altro Stato membro è disciplinato dalla direttiva CEE, 22 marzo 1977, 77/249/CEE e dalla direttiva del 16 febbraio 1998, 98/5/CE, attuata nell'ordinamento italiano con d.lgs. 2 febbraio 2001, n. 96, da cui emerge che la possibilità di ricevere un incarico occasionale da parte di un difensore che esercita la professione in un altro Stato membro prevede il presupposto dell'affiancamento di un avvocato dello Stato in cui si esegue l'attività giudiziaria. Sul tema, E. LORENZETTO, *L'assetto delle impugnazioni*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d. lgs. n.*

Riconosciuto, l'ordine è eseguito dall'autorità di esecuzione secondo le regole indicate dall'autorità di emissione, sempre che tali formalità e procedure non siano lesive dei principi fondamentali dello Stato di esecuzione⁹⁸⁶. In linea di principio, quindi, è il diritto dello Stato membro di emissione che disciplina la misura e che dovrebbe garantirne la successiva ammissibilità⁹⁸⁷.

Infine, l'art. 13 della direttiva 2014/41/UE dispone che l'autorità di esecuzione trasferisca senza indebito ritardo allo Stato di emissione le prove acquisite o già in possesso delle autorità competenti dello Stato di esecuzione dell'OEI⁹⁸⁸.

Nel solco di un "diritto di difendersi, impugnando"⁹⁸⁹, all'art. 14 della direttiva 2014/41/UE è previsto poi un sistema articolato di impugnazioni *ad hoc*. Mediante una clausola di equivalenza, il legislatore dell'Unione europea ha stabilito che gli Stati membri debbano prevedere mezzi di impugnazione equivalenti a quelli disponibili in un caso interno analogo per gli atti di indagine richiesti nell'OEI. Invece, per quanto attiene alle ragioni di merito sottese all'emissione dell'ordine, devono essere garantite impugnazioni introdotte mediante azioni nello Stato di emissione, fatti salvi le garanzie e i diritti fondamentali nello Stato di esecuzione⁹⁹⁰.

108 del 2017 (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 165; G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all'ordine europeo di indagine*, cit., p. 266. V. anche R. BELFIORE, *Su alcuni aspetti del decreto di attuazione dell'ordine europeo di indagine penale*, cit., p. 405.

⁹⁸⁶ Cfr., art. 9, par. 1 e 2, della direttiva 2014/41/UE. Per la procedura interna, v., art. 4, comma 2, d.lgs. 21 giugno 2017, n. 108.

⁹⁸⁷ Sul punto, M. DANIELE, *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, cit., p. 182; A. KLIP, *European Criminal Law. An Integrative Approach*, Cambridge, 2021, p. 395 ss.

⁹⁸⁸ Per la procedura interna, v., art. 12, d.lgs. 21 giugno 2017, n. 108.

⁹⁸⁹ Per tale espressione, E. LORENZETTO, *L'assetto delle impugnazioni*, cit., p. 151, nonché, volendo, A. GAUDIERI, *Opposizione al decreto di riconoscimento dell'ordine europeo di sequestro: scenari*, cit., p. 2026 ss.

⁹⁹⁰ Per un approfondimento sul sistema delle impugnazioni, R. BELFIORE, *Riflessioni a margine della direttiva sull'Ordine europeo di indagine penale*, cit., p. 3295 ss.; A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., p. 261; O. CALAVITA, *Ordine europeo di indagine e rimedi interni: riflessioni sulle prime applicazioni giurisprudenziali*, in *Leg. Pen.*, 30 settembre 2021, disponibile al link: <http://www.la-legislazione-penale.eu/ordine-europeo-di-indagine-e-rimedi-interni-riflessioni-sulle-prime-applicazioni-giurisprudenziali-oscar-calavita/>; L. CAMALDO, F. CERQUA, *La direttiva sull'ordine europeo di indagine penale: le nuove prospettive per la libera circolazione delle prove*, cit., p. 3512; M. DANIELE, *Opposizione al riconoscimento dell'ordine europeo di sequestro e decisione de plano: una nullità assoluta*, in *Sistema penale*, 18 febbraio 2020; M. DANIELE, *Ricerca e formazione della prova – Profili generali*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 473 ss.; ID., *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali*, in *Dir. Pen. Cont.*, 3, 2016, p. 69; A. FABBRICATORE, *L'opposizione al riconoscimento dell'ordine europeo di sequestro probatorio*, in *Dir. Pen. e Proc.*, 6, 2020, p. 798 ss.; R.M. GERACI, *Ordine europeo di indagine ricevuto dall'estero e rimedi impugnatori praticabili*, in *Cass. pen.*, 9, 2019, p. 3184 ss.; M. GIACOMETTI, S. NEVEU, *La décision d'enquête européenne: un nouvel instrument destiné à révolutionner la récolte de preuves au sein de l'UE?*, in *Revue de Droit pénal et de Criminologie*, 9-10, 2016, p. 899; R.E. KOSTORIS, *Ordine di investigazione europeo e tutela dei diritti fondamentali*, cit., p. 1444; E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, cit., p. 1306 ss.; ID., *Continua la saga dei vizi capitali: contraddittorio violato nell'opposizione al riconoscimento dell'ordine europeo di sequestro probatorio*, in *Cass. pen.*, 11, 2020, p. 4093 ss.; ID., *L'assetto delle impugnazioni*, cit., p. 157; S. MARCOLINI, *L'ordine europeo di indagine alla prova dei fatti: prime pronunce in materia*, cit., p. 3370 ss. Sullo stesso argomento, volendo, A. GAUDIERI, *Opposizione al decreto di riconoscimento dell'ordine europeo di sequestro: scenari*, cit., p. 2024 ss. Sul tema si è pronunciata anche la Corte di giustizia dell'Unione europea. Cfr., Corte di giustizia, sentenza 24 ottobre 2019, causa C-324/17, *Ivan Gavanov*. Per un commento alla sentenza, C. DE LUCA, *La prima pronuncia della Corte di giustizia sull'ordine europeo di indagine penale: un approccio formale diretto a favorire l'efficacia della*

Con l'art. 14, par. 4 della direttiva 2014/41/UE, gli Stati sono poi invitati ad assicurare che «i termini per l'impugnazione siano uguali a quelli previsti in casi interni analoghi e siano applicati in modo da garantire che il diritto a tale impugnazione possa essere esercitato efficacemente dalle persone interessate». Dunque, non si tratterebbe di un ulteriore ed autonomo *remedy*: la locuzione “*legal remedies*” – a differenza della classica espressione “*effective remedies*” – starebbe ad indicare che, qualora manchino nell'ordinamento interno impugnazioni o ricorsi di siffatta natura, allora anche le attività richieste con l'OEI potrebbero non essere oggetto di rimedi impugnatori⁹⁹¹.

Così delineato, il procedimento sembra particolarmente celere rispetto agli strumenti più risalenti. E a ben vedere, una conferma sarebbe ravvisabile nei termini particolarmente rigorosi per la formazione delle prove richieste.

L'art. 12 della direttiva 2014/41/UE prevede che l'adozione della decisione sul riconoscimento o sull'esecuzione, nonché il compimento dell'atto investigativo abbiano luogo con la massima celerità e priorità usate in un caso interno analogo. Nello specifico, la decisione sul riconoscimento o sull'esecuzione deve essere adottata entro trenta giorni, prorogabili fino ad un massimo di altri trenta; mentre, salvo non sussistano motivi di rinvio, l'atto di indagine è compiuto entro novanta giorni dalla decisione sul riconoscimento o sull'esecuzione, ma, qualora non sia possibile rispettare tale termine, l'autorità di esecuzione potrà individuare un momento più appropriato, previa consultazione con l'autorità di emissione⁹⁹².

La procedura, dunque, dovrebbe durare in media dai 60 ai 120 giorni circa. Il dato è confortato anche dalla recente relazione svolta dalla Commissione europea, in cui si attesta che la maggior parte degli Stati membri ha riferito di aver dato esecuzione a un ordine europeo di indagine e trasferito le prove allo Stato di emissione entro 30-61 giorni; mentre un ampio numero di Stati membri ha riferito di aver ricevuto le prove dallo Stato di esecuzione entro 91-120 giorni⁹⁹³.

Sebbene i termini siano particolarmente stringenti, la dottrina – così come anche gli organi dell'Unione europea – ritiene che non siano idonei a soddisfare le esigenze di celerità delle investigazioni digitali, pur potendo queste ultime essere oggetto di un ordine europeo di indagine⁹⁹⁴.

Invero, la volatilità del dato informatico mal si concilia con le tempistiche dello strumento. Pur verificandosi una apprezzabile diminuzione dei tempi rispetto ai classici strumenti rogatoriali basati sul principio della mutua assistenza, l'ordine europeo di indagine non riesce a garantire una tempestiva apprensione del dato elettronico che in ogni caso rischia di andare disperso. Il rischio pericolo di distruzione del dato è

cooperazione giudiziaria, in *Cass. pen.*, 10, 2020, p. 3854 ss.; M. SIMONATO, *Reciproco riconoscimento in materia penale e vie di ricorso: la prima sentenza della CGUE sull'ordine europeo di indagine*, in *europeanlawblog.it*, 1 aprile 2020.

⁹⁹¹ Sul punto, A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., p. 261 ss.; R. DEL COCO, *Ordine europeo di indagine e poteri sanzionatori del giudice*, cit., p. 8. L.'A. osserva che la disciplina dell'OEI non ha né garantito la reciproca ammissione delle prove, né ha previsto «un sistema unitario e condiviso di sanzioni che garantiscano l'effettività di una tutela multilivello delle garanzie».

⁹⁹² La disciplina interna, all'art. 4, d.lgs. 21 giugno 2017, n. 108, ha sostanzialmente recepito le stesse disposizioni, individuando i termini, così come indicati dall'art. 12 della direttiva 2014/41/UE.

⁹⁹³ Cfr., *Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della direttiva 2014/41/UE del Parlamento e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale*, Bruxelles, 20 luglio 2021, COM(2021) 409 final, p. 13.

⁹⁹⁴ Così, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 173.

particolarmente alto, tant'è che, una volta ricercato, spesso non è acquisibile perché ormai è troppo tardi.

Sebbene possa essere utilizzato per tutti gli atti di indagine finalizzati all'acquisizione della prova, lo strumento non appare pienamente idoneo ad essere impiegato per le prove informatiche⁹⁹⁵, perché l'assenza di una disciplina *ad hoc* e di settore⁹⁹⁶ lascerebbe trasparire un *deficit* normativo di estrema rilevanza.

È pur vero che l'autorità giudiziaria può indicare precise modalità di esecuzione delle operazioni di acquisizione della prova elettronica, richiedendo il rispetto di procedure e protocolli⁹⁹⁷; tuttavia, la soluzione – invero, portatrice di ampia discrezionalità in capo all'autorità legittimata – appare insoddisfacente perché, per l'appunto, determinerebbe operazioni estremamente lente, poco uniformi ed incostanti⁹⁹⁸, se solo si tiene conto anche dei tempi generalmente impiegati per le procedure relative agli ordini europei di indagine.

La scelta di prevedere disposizioni “supplementari” ovvero di lasciare agli Stati la possibilità di decidere in accordo “modalità pratiche”, così da conciliare le differenze esistenti tra i diritti nazionali di tali Stati⁹⁹⁹, rappresenta una chiara scelta legislativa finalizzata a tutelare al meglio i diritti fondamentali, laddove l'interferenza si fa più massiccia. L'area della prova elettronica è sicuramente annoverabile tra quelle in cui l'impatto sui diritti fondamentali è maggiore, per cui, probabilmente, bisognava agire in tal senso, prevedendo una disciplina di settore o un vero e proprio “modello europeo d'indagine”.

In generale, la maggior parte degli Stati membri – così come Eurojust e la Rete giudiziaria europea – ritiene che la direttiva abbia semplificato e accelerato l'acquisizione delle prove e abbia avuto un impatto positivo sulla cooperazione giudiziaria in materia penale. Il quadro attuale per il riconoscimento reciproco degli ordini europei di indagine per l'ottenimento delle prove è considerato soddisfacente dalla maggior parte degli Stati membri.

⁹⁹⁵ Cfr., Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni “*Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025*, Bruxelles, 14 aprile 2021, COM(2021) 170 final, secondo cui l'ordine europeo di indagine, così come altri strumenti, sono stati concepiti per le prove fisiche e non sono completamente adeguati al mondo digitale, il che può ostacolare o rallentare le indagini e le azioni penali, poiché i dati non sono disponibili o accessibili in modo tempestivo.

⁹⁹⁶ Come, ad esempio, fatto per determinati atti: il trasferimento temporaneo delle persone detenute; l'audizione mediante videoconferenza o altra trasmissione audiovisiva; l'audizione mediante teleconferenza; l'acquisizione di informazioni e documenti presso banche e istituti finanziari; le operazioni sotto copertura; il ritardato arresto o sequestro, le intercettazioni di telecomunicazioni, incluse quelle telematiche e, infine, i provvedimenti di sequestro probatorio. Al contrario, l'ordine europeo di indagine penale non potrà esser emesso per costituire squadre investigative comuni e per i sequestri diversi da quello probatorio. Per uno studio sulle tecniche di investigazione definite “speciali”, che tiene conto del bilanciamento tra esigenze di accertamento e delle garanzie individuali, G. BARROCU, *Le speciali tecniche di investigazione nel contesto europeo*, in *Cass. pen.*, 3, 2020, p. 1325 ss.

⁹⁹⁷ In tal senso, A. COLAIOCCO, *La rilevanza delle best practices nell'acquisizione della digital evidence alla luce delle novità sulla cooperazione giudiziaria*, cit., p. 8; M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul D.Lgs. n. 108 del 2017*, cit., p. 213.

⁹⁹⁸ Vi è chi ha osservato che sussiste un alto rischio di non corretta acquisizione e conservazione dei dati digitali, sia per la difficoltà nella formazione del dato, sia per la possibilità che nei vari Stati possano essere adottati procedure e *standard* disomogenei. In tal senso, N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, cit., p. 700.

⁹⁹⁹ Cfr., considerando n. 24 della direttiva 2014/41/UE. Sul punto, inoltre, F. SIRACUSANO, *La prova informatica transnazionale: un difficile “connubio” fra innovazione e tradizione*, cit., p. 188.

Purtuttavia, lo stesso sentimento non si prova quando si restringe il campo d'indagine alle prove elettroniche, in relazione alle quali gli Stati membri continuano a segnalare la necessità di norme specifiche, tanto più pressanti in ragione dell'aumento della digitalizzazione e della pandemia di Covid-19¹⁰⁰⁰.

La necessità di una specifica disciplina si evince dalle particolari caratteristiche assunte dal dato elettronico, nonché dai diritti fondamentali coinvolti. Una ricerca di tali informazioni permette alle autorità giudiziarie degli Stati di infiltrarsi profondamente nella vita delle persone. Le conseguenze sembrano evidenti: ad una maggior invasività dello strumento corrisponde un più alto rischio di lesione degli interessi individuali e dei diritti fondamentali, con conseguente riduzione della dignità delle persone.

Se è vero, allora, che il legislatore europeo ha deciso di prevedere una specifica disciplina per le intercettazioni, in ragione di uno strumento ritenuto particolarmente intrusivo della sfera privata ed intima della persona, allora sembrerebbe necessario prevedere una disciplina di settore specifica per la formazione di prove elettroniche conservate nei *server* degli *internet service provider* e che tenga conto sia degli interessi dei singoli, sia degli interessi pubblici alla repressione dei reati, sia delle specificità dell'*e-evidence*.

3. L'inadeguatezza dell'ordine europeo di indagine: verso una disciplina dell'*e-evidence* transfrontaliera nello spazio di libertà, sicurezza e giustizia

L'inadeguatezza dell'ordine europeo di indagine penale appare evidente a causa delle problematiche specifiche sorte in relazione alla prova elettronica. Le cause – come appena illustrato – sono molteplici e tali da aver spinto i tecnici del diritto a percorrere territori sinora inesplorati.

L'ordine europeo di indagine si dimostra lento rispetto alle istanze di sicurezza mosse contro i reati di maggior allarme sociale¹⁰⁰¹. Al tempo stesso, esso appare infruttuoso perché non utilizzabile nei confronti di tutti gli Stati membri¹⁰⁰² e inidoneo perché non raggiunge l'obiettivo di acquisire prove caratterizzate da estrema volatilità.

Né appare efficace la procedura d'urgenza prevista dall'art. 12, par. 2 della direttiva 2014/41/UE¹⁰⁰³, perché l'adempimento delle formalità richieste appare particolarmente difficoltoso, a partire dall'onere di traduzione del modello *standard*¹⁰⁰⁴.

¹⁰⁰⁰ Cfr., *Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della direttiva 2014/41/UE del Parlamento e del Consiglio, del 3 aprile 2014, relativa all'ordine europeo di indagine penale*, Bruxelles, 20 luglio 2021, COM(2021) 409 final, p. 13. Anche in dottrina sembrerebbe condivisa l'idea di un ordine europeo d'indagine inadeguato rispetto al fenomeno dell'*e-evidence*. Sul punto, A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova elettronica*, in AA.VV., *Mobilità, sicurezza e nuove frontiere tecnologiche* (a cura di V. MILITELLO, A. SPENA), Torino, 2018, p. 421 ss.

¹⁰⁰¹ In tal senso, F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., disponibile al link: <https://www.magistraturaindipendente.it/lordine-di-produzione-e-di-conservazione-europeo-delle-prove-elettroniche.htm>. V. inoltre, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 5, 2018, p. 280.

¹⁰⁰² Ad esempio, all'ordine europeo di indagine non ha aderito l'Irlanda, sede di alcune delle più grandi società che gestiscono dati elettronici.

¹⁰⁰³ Per la disciplina interna, v., art. 4, comma 3, d.lgs. 21 giugno 2017, n. 108.

¹⁰⁰⁴ Sul punto, D. CURLOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 6, 2021, p.

L'inadeguatezza dello strumento è stata riconosciuta anche dalla Commissione per le libertà civili, la giustizia e gli affari interni. Infatti, in un rapporto relativo al progetto di Regolamento relativo agli ordini europei di produzione e di conservazione delle prove elettroniche ha affermato che occorre lavorare a norme specifiche per quanto riguarda la cooperazione giudiziaria transfrontaliera per preservare e produrre informazioni elettroniche, al fine di integrare la vigente legislazione dell'Unione europea e di chiarire le norme sulla cooperazione tra le autorità giudiziarie e di contrasto e i prestatori di servizi nel settore delle informazioni elettroniche, garantendo al contempo il pieno rispetto dei diritti fondamentali e dei principi riconosciuti dall'articolo 6 TUE e dalla Carta dei diritti fondamentali dell'Unione europea, nonché dello Stato di diritto¹⁰⁰⁵.

Insomma, il coro è unanime nell'affermare che si è di fronte ad un quadro giuridico europeo perfettibile, poiché non sono disciplinati in modo omogeneo la ricerca, la conservazione e lo scambio delle prove elettroniche tra gli Stati membri dell'Unione europea, sebbene siano stati compiuti notevoli progressi in detta direzione negli ultimi anni¹⁰⁰⁶. Regna la frammentarietà, con conseguente confusione dei prestatori di servizi che cercano di ottemperare alle richieste di servizi di contrasto alla criminalità.

Un simile contesto ha consentito lo sviluppo della *voluntary disclosure* anche sul territorio dell'Unione europea. Per prassi, le autorità giudiziarie inviano richieste dirette ai prestatori di servizi¹⁰⁰⁷, senza un previo coinvolgimento di altri Stati, *bypassando* così le discipline lente e inefficienti. Di conseguenza, i prestatori decidono di volta in volta se collaborare e secondo quali limiti¹⁰⁰⁸, finendo per assumere il ruolo di «veri depositari del

753 ss. L'A. ritiene anche che «il requisito della reciprocità presenta punti critici al cospetto della prova digitale. Esiste, infatti, un'evidente difficoltà di armonizzazione dei criteri di ammissibilità e valutazione della prova digitale tra gli Stati i quali presentano, alle volte, regole e pratiche molto diverse: scarsa uniformità nel tipo di attività investigativa concretamente esperibile, marcata disomogeneità di procedure e *standard* operativi in punto di acquisizione e conservazione di dati digitali, significativi ritardi di adeguamento di alcune legislazioni rispetto alle modifiche repentine prodotte dal progresso tecnologico, difformità di approccio nella misura del bilanciamento tra i molteplici diritti messi in gioco, quelli dei soggetti coinvolti nel procedimento penale (diritto alla protezione dei dati personali; rispetto della vita privata e familiare; libertà di espressione; diritto alla difesa; diritto ad un processo equo), quelli dei prestatori di servizio (diritto alla libertà d'impresa) e, più in generale, quelli di tutti i cittadini dello spazio europeo (il diritto alla libertà e alla sicurezza), ecc.».

¹⁰⁰⁵ Cfr., Commissione per le libertà civili, la giustizia e gli affari interni, *Relazione sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, A9-0256/2020.

¹⁰⁰⁶ Va, inoltre, considerato che all'interno dell'Unione europea, le norme sulle prove variano notevolmente tra le giurisdizioni, anche tra Paesi con tradizioni giuridiche simili. In termini generali, gli ordinamenti giuridici appartenenti alla tradizione di *common law* tendono ad avere regole definite in merito all'ammissibilità delle prove. Negli ordinamenti giuridici della tradizione del diritto continentale, in cui i giudici mantengono un alto grado di controllo sui procedimenti giudiziari, l'ammissibilità delle prove può essere flessibile, sebbene la valutazione di esse (compreso l'accertamento relativo alla loro credibilità e autenticità) possa anche obbedire a un insieme completo di regole. Sul punto, L. BUONO, *The genesis of European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, in *ERA Forum*, 19, 2019, p. 308.

¹⁰⁰⁷ Sul rapporto con i soggetti terzi, tra cui i fornitori di servizi, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 181 ss.

¹⁰⁰⁸ Così, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1282; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 281; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 4.

potere di attuazione dell'orizzonte investigativo»¹⁰⁰⁹. Anche tale soluzione alternativa di accesso ai dati digitali aventi attitudine probatoria appare insoddisfacente.

La frammentazione giuridica e le prassi che ne sono scaturite hanno di fatto generato incertezza giuridica e obblighi contrastanti. Inoltre, in discussione vi è la protezione dei diritti fondamentali e delle garanzie procedurali delle persone interessate¹⁰¹⁰.

Solo per dare un dato, nello spazio di libertà, sicurezza e giustizia meno della metà delle richieste probatorie agli *internet service providers* sono evase con esito positivo ed almeno due terzi dei reati, nei confronti dei quali appare necessaria una formazione della prova digitale all'estero per essere provati, non sono perseguiti efficacemente¹⁰¹¹.

La situazione attuale – nel contesto dell'Unione europea – non appare particolarmente fulgida: mancano la trasparenza e una cooperazione affidabile con i fornitori di servizi; vi sono dubbi circa la competenza giurisdizionale per gli atti di indagine.

Se si considera che oltre la metà delle indagini penali comprende una richiesta di accesso transfrontaliero a prove elettroniche, appare necessario introdurre strumenti europei vincolanti per l'acquisizione e la consultazione di dati che rendano più facile e più rapido l'accesso delle autorità di polizia e giudiziarie al materiale probatorio elettronico ritenuto indispensabile per le indagini finalizzate all'arresto e alla condanna di criminali e terroristi¹⁰¹².

Infatti, migliorare l'accesso transfrontaliero alle prove elettroniche è una questione urgente che riguarda quasi tutti i tipi di reato¹⁰¹³. In particolare, il fenomeno degli attentati terroristici ha evidenziato la necessità, in via prioritaria, di trovare nuovi modi per garantire e ottenere prove elettroniche in modo più rapido ed efficace.

La complessità del tema – che coinvolge un'ampia gamma di interessi, diritti e garanzie – non poteva essere risolta dai singoli Stati membri, per cui l'Unione europea sembra essere il livello più adeguato a risolvere i problemi individuati.

La piena consapevolezza di un fenomeno di difficile lettura e di una situazione particolarmente complessa risultò chiara già al tempo dell'adozione della direttiva 2014/41/UE sull'ordine europeo di indagine, quando si cominciò a discutere di una legislazione *ad hoc*.

Nel 2013, la Commissione già intuì che l'Unione europea e gli Stati membri avessero bisogno di una legislazione solida ed efficace per affrontare il cybercrimine. Era, dunque,

¹⁰⁰⁹ Per questa espressione, S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 182.

¹⁰¹⁰ Ritiene la prassi della *voluntary disclosure* lesiva del diritto di difesa delle persone sia fisiche sia giuridiche, G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), cit., p. 1013 ss.

¹⁰¹¹ Per tale dato, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 281.

¹⁰¹² Cfr., *Parere del Comitato economico e sociale europeo sulla «Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale» e sulla «Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali»*, 12.7.2018, in GUUE C-367, del 10 ottobre 2018.

¹⁰¹³ Cfr., *Commission staff working document, Impact - Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, 17 aprile 2018, SWD(2018) 118 final, p. 6.

avvertito come necessario dotare le autorità di strumenti efficienti e non datati idonei a combattere il crimine con strumenti operativi di ultima generazione¹⁰¹⁴.

Nello stesso anno, nell'ambito del progetto congiunto *CyberCrime@IPA*, l'Unione europea ed il Consiglio d'Europa pubblicarono la “*Electronic evidence – A basic guide for police officers, prosecutors ad judges*”, ove emergeva che i casi riguardanti prove elettroniche archiviate su sistemi informatici o altri dispositivi erano in netto aumento ed era necessario agire nella formazione degli operatori.

Infatti, nella maggior parte dei casi, questi incontrano difficoltà nell'affrontare le nuove realtà del mondo cibernetico e necessitano di essere formati alla conoscenza e alla comprensione della criminalità informatica e delle prove elettroniche¹⁰¹⁵.

Intanto, nel 2014, l'Ufficio europeo per la lotta antifrode (OLAF) ha pubblicato le “*Guidelines on digital forensic procedures for OLAF Staff*”, a conferma che il tema delle investigazioni digitali e della formazione della prova digitale nello spazio di libertà, sicurezza e giustizia aveva ormai assunto centralità¹⁰¹⁶.

È però nel 2015 che le attività verso una uno strumento utile per la formazione della prova elettronica transfrontaliera hanno avuto una decisa accelerazione.

Nell'Agenda europea sulla sicurezza¹⁰¹⁷, la Commissione sottolineava come «la criminalità informatica è per sua natura senza frontiere, flessibile e innovativa. Nel prevenire, individuare e perseguire i reati informatici, le autorità di contrasto devono essere in grado di eguagliare e anticipare l'ingegno dei criminali. La criminalità informatica esige che le autorità giudiziarie competenti ripensino al modo in cui cooperano nell'ambito delle loro giurisdizioni e della legge applicabile per garantire un accesso transfrontaliero più rapido alle prove e alle informazioni, tenendo conto degli sviluppi tecnologici attuali e futuri, quali il *cloud computing* e l'“internet delle cose”. La raccolta delle prove elettroniche in tempo reale da altre giurisdizioni su questioni quali i proprietari di indirizzi IP o altre prove elettroniche, e la loro ammissibilità dinanzi al giudice sono questioni di importanza fondamentale. È inoltre necessario che il personale

¹⁰¹⁴ In tal senso, *Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni – Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, Bruxelles, 7 febbraio 2013, JOIN(2013) 1 final, p. 10.

¹⁰¹⁵ La guida è disponibile al seguente link: <https://www.coe.int/en/web/cybercrime/trainings>.

¹⁰¹⁶ Le Linee guida sono state poi riviste. La nuova versione è del 15 febbraio 2016. Le linee guida dell'OLAF sulle procedure digitali forensi sono regole interne che possono essere seguite dal personale dell'OLAF per quanto riguarda l'identificazione, l'acquisizione, la raccolta, l'analisi e la conservazione delle prove digitali. Lo scopo di queste linee guida è quello di stabilire le regole per condurre le operazioni di *digital forensic* in modo da garantire l'integrità e la catena delle prove da ammettere nei vari procedimenti.

Lo scopo di un'operazione di *digital forensic* è quello di proteggere potenziali prove digitali pertinenti per un'indagine dell'OLAF. Poiché le operazioni di *digital forensic* comportano spesso la raccolta di grandi quantità di dati, compresi i dati personali, possono essere invasive della *privacy*. Queste linee guida, quindi, sono state concepite anche per aiutare a garantire il rispetto della protezione dei dati nel contesto delle operazioni di *digital forensic* e completano le *Instructions to Staff on Data Protection* (ISDP).

Queste linee guida prendono in considerazione *standard* e buone pratiche approvate a livello internazionale come lo standard ISO:27037 sulle “Linee guida per l'identificazione, raccolta, acquisizione e conservazione delle prove digitali”, adottato nell'ottobre 2012, e la “Good practice guide for digital evidence” pubblicata dalla UK Association of Chief Police Officers (APCO) nel marzo 2012.

Le linee guida dell'OLAF sono consultabili al seguente link: https://ec.europa.eu/anti-fraud/system/files/2021-07/guidelines_en_bb84583638.pdf.

¹⁰¹⁷ Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni “*Agenda europea sulla sicurezza*”, Strasburgo, 28 aprile 2015, COM(2015) 185 final.

delle autorità di contrasto sia altamente qualificato, in grado di tenere il passo con l'aumento considerevole della portata, della sofisticazione e dei tipi di reati informatici».

Intanto, la stagione degli attentati ha fatto sì che, nel 2016, i ministri della giustizia e degli interni dell'UE con una dichiarazione congiunta abbiano affermato che sia prioritario trovare «modalità per assicurare e ottenere più rapidamente ed efficacemente prove digitali, intensificando la cooperazione con i Paesi terzi e con i fornitori di servizi operanti nel territorio europeo, al fine di migliorare la conformità con la legislazione dell'UE e degli Stati membri e i contatti diretti con le autorità incaricate dell'applicazione della legge»¹⁰¹⁸.

A seguito di tale dichiarazione, la Commissione, nell'invitare tutta l'Unione europea e i singoli Stati ad abbracciare un concetto di tutela della sicurezza collettiva di tutta l'Unione, constatato che non esiste un approccio armonizzato sulle modalità di accesso alle informazioni digitali, ha intensificato i suoi sforzi al fine di produrre un testo legislativo nel minor tempo possibile e sottoporlo all'attenzione del Parlamento europeo e del Consiglio¹⁰¹⁹, ricevendo il supporto del Consiglio dell'Unione europea.

Invero, con le conclusioni sul miglioramento della giustizia penale nel cyberspazio, il Consiglio dell'Unione europea ha invitato la Commissione a intraprendere azioni per migliorare la cooperazione con i fornitori di servizi, rendere più efficiente l'assistenza giudiziaria reciproca e proporre soluzioni ai problemi di determinazione e applicazione della giurisdizione nel cyberspazio¹⁰²⁰.

Nel 2017, ci fu la svolta sul fronte del dialogo interistituzionale. Al Consiglio "Giustizia e affari interni" dell'8 e 9 giugno, i ministri della giustizia e degli affari interni discussero la via da seguire in materia di prove elettroniche sulla base delle soluzioni pratiche individuate a seguito della procedura di consultazione di esperti da parte della Commissione. A larga maggioranza, si sostenne che occorre una iniziativa legislativa dell'Unione europea riguardo alla cooperazione diretta con i fornitori di servizi e alla definizione di condizioni comuni e requisiti minimi in ambito UE per l'accesso diretto ai dati da parte delle autorità a partire da un sistema informatico, tenendo in debito conto le questioni inerenti alla protezione dei dati e, di conseguenza, dei diritti fondamentali¹⁰²¹.

Intanto, al Consiglio europeo del 22 e 23 giugno 2017, incentrato sul rafforzamento dell'Europa e la protezione dei suoi cittadini mediante misure efficaci volte a combattere il terrorismo nonché a sviluppare la sicurezza e la difesa comuni, si è ritenuto che l'effettivo accesso alle prove elettroniche sia essenziale per combattere le gravi forme di

¹⁰¹⁸ *La Dichiarazione comune dei ministri della giustizia e degli interni dell'UE e dei rappresentanti delle istituzioni dell'UE sugli attentati terroristici di Bruxelles del 22 marzo 2016*, pubblicata il 24 marzo 2016, è disponibile al seguente link: <https://www.consilium.europa.eu/it/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/>. In dottrina, A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 46.

¹⁰¹⁹ Cfr. Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo e al Consiglio "Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per l'Unione della sicurezza", Bruxelles, 20 aprile 2016, COM(2016) 230 final; Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni "Programma di lavoro della Commissione per il 2017. Realizzare un'Europa che protegge, dà forza e difende", Strasburgo, 25 ottobre 2016, COM (2016) 710 final, § 7.

¹⁰²⁰ Cfr., *Conclusioni del Consiglio dell'Unione europea sul miglioramento della giustizia penale nel cyberspazio*, Lussemburgo, 9 giugno 2016, ST9579/16, disponibile al link: <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>.

¹⁰²¹ Per i risultati del Consiglio "Giustizia e affari interni" dell'8 e 9 giugno 2017, <https://www.consilium.europa.eu/it/meetings/jha/2017/06/08-09/#>. Cfr., anche, *Documento del Consiglio UE*, 14435/17, del 20 novembre 2017; *Documento del Consiglio UE*, 15748/17, del 12 dicembre 2017.

criminalità e il terrorismo e che, fatte salve le garanzie adeguate, occorre assicurare la disponibilità dei dati¹⁰²².

Dal proprio canto, il Parlamento europeo – nel sottolineare che un approccio comune europeo alla giustizia penale nel ciberspazio è prioritario, in quanto consentirà di migliorare l'applicazione dello stato di diritto nel ciberspazio e agevolare l'ottenimento di prove elettroniche nei procedimenti penali, oltre a contribuire alla conclusione delle cause molto più velocemente di quanto sia possibile oggi – ha comunque posto l'attenzione sulla necessità di un quadro in materia di prove elettroniche che comprenda garanzie sufficienti per i diritti e le libertà di tutti gli interessati¹⁰²³.

Il passo definitivo verso la produzione di una proposta da presentare al Parlamento europeo e al Consiglio avvenne a seguito delle consultazioni, avviate nel luglio 2017, mediante un questionario¹⁰²⁴ e che hanno coinvolto i maggiori fornitori di servizi internet, rappresentanti di organizzazioni governative e non governative ed altri portatori di interessi.

Il questionario ha rivelato che non esisteva un approccio comune per ottenere l'accesso transfrontaliero alle prove elettroniche per il quale ciascuno Stato membro aveva sviluppato la propria prassi interna, bensì, col tempo, si erano sedimentati una serie di approcci diversi tra loro, principalmente a causa della mancanza di un quadro giuridico comune per l'ottenimento delle prove elettroniche, che crea incertezza giuridica ed evidenti ostacoli alle indagini transfrontaliere.

Di conseguenza, venne presentato un dettagliato documento tecnico – non adottato né omologato dalla Commissione europea – ove si affermava che un quadro comune tra gli Stati membri potrebbe fornire una base giuridica efficiente e riconoscere la legalità delle attuali pratiche di cooperazione diretta. Così, le forze dell'ordine e le autorità giudiziarie di uno Stato membro si doterebbero delle competenze necessarie per presentare richieste di produzione non vincolanti per l'accesso transfrontaliero alle prove elettroniche, consentendo ai fornitori di servizi con sede in un altro Stato di divulgare prove elettroniche alle autorità estere sulla base di tale richiesta di produzione, senza passare per le forze dell'ordine o le autorità giudiziarie dello Stato in cui hanno sede¹⁰²⁵. Si

¹⁰²² Cfr., *Conclusioni del Consiglio europeo*, 22-23 giugno 2017, EUCO 8/17. V., inoltre, *Conclusioni del Consiglio europeo*, 19 ottobre 2017, EUCO 14/17. Il dialogo tra istituzioni nel 2017 fu di ampio respiro nonché particolarmente fruttuoso e proficuo.

¹⁰²³ Cfr., *Risoluzione del Parlamento europeo del 3 ottobre 2017 sulla lotta alla criminalità informatica*, 2017/2068(INI). Il Parlamento europeo ha anche sottolineato che il nuovo strumento per le prove elettroniche deve comprendere un requisito in base al quale le richieste di prove elettroniche siano trasmesse in primo luogo ai titolari del trattamento dei dati o ai proprietari dei dati, al fine di assicurare il rispetto dei loro diritti, nonché dei diritti di coloro cui i dati fanno riferimento (per esempio il loro diritto di far valere il segreto professionale forense e di presentare ricorso in caso di accesso sproporzionato o altrimenti illecito). Inoltre, ha sottolineato la necessità di garantire che eventuali quadri giuridici tutelino i prestatori di servizi e tutte le altre parti dalle richieste che possano creare conflitti di leggi o altrimenti pregiudicare la sovranità di altri Stati.

¹⁰²⁴ Il questionario, con le relative informazioni di dettaglio sulle consultazioni, sono disponibili al seguente link: https://ec.europa.eu/info/consultations/public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en. I risultati delle consultazioni sono disponibili al seguente link: https://ec.europa.eu/info/publications/position-papers-2017-public-consultation-improving-cross-border-access-electronic-evidence-criminal-matters_en.

¹⁰²⁵ Si tratta del documento tecnico *Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, disponibile al link: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf. In

gettarono così le basi per l'ordine europeo di produzione: la Commissione era pronta a presentare una proposta legislativa ufficiale in materia di *e-evidence*, attività che poi effettivamente fece nel 2018¹⁰²⁶.

Ed infatti, il 17 aprile 2018, la Commissione ha presentata un “pacchetto” di proposte relative alla prova elettronica transnazionale: la proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale¹⁰²⁷ e la proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali¹⁰²⁸.

Il 18 ottobre 2018 il Consiglio europeo ha chiesto di trovare soluzioni per garantire un accesso transfrontaliero rapido ed efficiente alle prove elettroniche al fine di combattere efficacemente il terrorismo e altre forme gravi di criminalità, sia all'interno dell'UE che a livello internazionale. Ha inoltre sottolineato che si dovrebbe giungere a un accordo sulle proposte della Commissione riguardanti le prove elettroniche entro la fine dell'attuale legislatura¹⁰²⁹.

Il negoziato è stato avviato nell'ambito del gruppo di lavoro COPEN (*Working party on Cooperation in Criminal matters*)¹⁰³⁰ ed attualmente entrambe le proposte sono in fase di trilogia tra la Commissione europea, Consiglio UE e Parlamento europeo.

Tenuto conto dello stato attuale del procedimento di formazione degli atti normativi, ai fini del presente lavoro si considereranno i testi dell'orientamento generale. Infatti, esistono due versioni del testo: la proposta originale della Commissione e l'orientamento generale del Consiglio. Quest'ultima versione mira a risolvere delle problematiche sorte, ma gli elementi fondamentali della struttura dell'ordine rimangono immutati.

4. Gli ordini europei di produzione e conservazione: la scelta della fonte normativa

Come sinora descritto, l'Unione europea ha avvertito la forte necessità di affrontare le nuove sfide dell'era digitale con strumenti all'avanguardia, idonei a combattere una

dottrina, inoltre, L. BUONO, *The genesis of European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, cit., p. 309.

¹⁰²⁶ Cfr., Comunicazione congiunta al Parlamento europeo e al Consiglio “*Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*”, Bruxelles, 13 settembre 2017, JOIN(2017) 450 final, p. 15. Nella medesima comunicazione, la Commissione ha sottolineato che indagare e perseguire efficacemente i reati favoriti dalla cibernetica costituisce un deterrente essenziale dei ciberattacchi, e che il quadro procedurale attuale deve essere adattato meglio all'era di internet. Talvolta le procedure non sono risultate adeguate alla velocità dei ciberattacchi, che richiedono una rapida cooperazione transfrontaliera. V., inoltre, il *Working document for the Joint Declaration on the EU's legislative priorities for 2018 - 19, 31 new initiatives for a More United, Stronger and More Democratic Union* della Commissione europea, disponibile al link: https://ec.europa.eu/info/sites/default/files/working-document-joint-declaration-legislative-priorities-2018-19_en.pdf.

¹⁰²⁷ Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, Strasburgo, 17 aprile 2018, COM/2018/225 final - 2018/0108 (COD).

¹⁰²⁸ Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali, Strasburgo, COM/2018/226 final - 2018/0107 (COD).

¹⁰²⁹ *Conclusioni del Consiglio europeo*, 18 ottobre 2018, EUCO 13/18.

¹⁰³⁰ Così, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 62.

criminalità evoluta ed in continuo mutamento. Il fenomeno digitale entra a pieno nei gangli della società mondiale ed europea, mutandola.

Preso atto del fenomeno che ormai coinvolge ogni aspetto della vita, l'Unione europea ha deciso di adattare i meccanismi di cooperazione giudiziaria in materia penale, affrontando, *inter alia*, lo specifico problema della natura volatile delle prove elettroniche e della loro dimensione transnazionale.

Al già nutrito ventaglio di ordini utilizzati quotidianamente nello spazio di libertà, sicurezza e giustizia per combattere la criminalità¹⁰³¹, si affiancheranno due nuovi strumenti: l'ordine europeo di produzione e l'ordine europeo di conservazione¹⁰³².

¹⁰³¹ Tra questi, a titolo esemplificativo, possiamo annoverare l'ordine europeo di indagine, introdotto con la direttiva 2014/41/UE, l'ordine europeo di protezione, previsto dalla direttiva 2011/99/UE, l'ordine europeo di rimozione, creato con il Regolamento (UE) 2021/784, i provvedimenti di congelamento e confisca, di cui al Regolamento (UE) 2018/1805, l'ordine di sorveglianza europeo, regolato dalla decisione quadro 2009/829/GAI ed il mandato di arresto europeo, disciplinato dalla decisione quadro 2002/584/GAI, che rappresenta l'archetipo degli ordini europei. Sul mandato di arresto europeo quale strumento basato sullo schema dell'ordine, P. TROISI, voce *Mandato di arresto europeo*, in *Treccani – Diritto on line*, 2014, disponibile al seguente link: [https://www.treccani.it/enciclopedia/mandato-di-arresto-europeo_\(Diritto-online\)/](https://www.treccani.it/enciclopedia/mandato-di-arresto-europeo_(Diritto-online)/). V., inoltre, M. BARGIS, *Libertà personale e consegna*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019 p. 359, secondo cui il mandato di arresto europeo «rappresenta il primo e a tutt'oggi il più importante strumento di mutuo riconoscimento per gli Stati membri dell'Unione europea»; S. MONTALDO, *Mandato d'arresto europeo, principio del reciproco riconoscimento e diritti del condannato*, in *Diritti umani e diritto internazionale*, 1, 2013, p. 226 ss.; S. MONTALDO, L. GROSSIO, *La riforma della disciplina di recepimento del mandato di arresto europeo: il nuovo assetto dei limiti all'esecuzione della richiesta di consegna*, in *Rivista Freedom, Security & Justice: European Legal Studies*, 3, 2021, p. 95 ss.

¹⁰³² Sulla proposta di Regolamento relativo agli ordini di produzione e conservazione di prove elettroniche in materia penale, B.J. BLAŽIČ, T. KLOBUČAR, *Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society*, in *Information & Communication Technology Law*, 1, 2020, p. 66 ss.; C. BRIÈRE, *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, in *European Papers*, 1, 2021, p. 493 ss.; L. BUONO, *The genesis of European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, cit., p. 307 ss.; O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *Leg. Pen.*, 30 marzo 2021, p. 1 ss.; H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, in *European Papers*, 1, 2021, p. 423 ss.; E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2722 ss.; M. CORHAY, *Private Life, Personal Data Protection and Role of Service Providers: the EU e-Evidence Proposal*, in *European Papers*, 1, 2021, p. 441 ss.; D. CURLOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora)*, cit., p. 745 ss.; M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1277 ss.; G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), cit., p. 1013 ss.; R. FLOR, *Cybercriminality: le foti internazionali ed europee*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019, p. 134 ss.; V. FRASSEN, *The European Commission's e-Evidence Proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?*, in www.europeanlawblog.eu, 12 ottobre 2018; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, in *Cass. pen.*, 3, 2019, p. 1340 ss.; S. DEPAUW, *Electronic Evidence in Criminal Matters: How About E-Evidence Proposal*, in *European Criminal Law Review*, 1, 2018, p. 62 ss.; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 277 ss.; L. GÓMEZ AMIGO, *Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima*, in *Revista Española de Derecho Europeo*, 71, 2019,

Per quanto attiene all'oggetto, il Regolamento affronta per la prima volta in maniera specifica il tema della prova elettronica¹⁰³³. Le norme che disciplineranno gli strumenti consentiranno alle autorità di uno Stato membro di ingiungere ad un prestatore di servizi che offre servizi nell'Unione europea di produrre o di conservare elementi elettronici, indipendentemente dal luogo in cui i dati sono collocati, senza però imporre a questi di acquisire o conservare sistematicamente dati diversi da quelli già raccolti per motivi aziendali o per rispettare altri obblighi di legge¹⁰³⁴.

Si tratterebbe, dunque, di strumenti utilizzabili unicamente per la ricerca e la formazione di prove elettroniche "estere", attraverso un canale di cooperazione rapida ed efficace con chi detiene i dati¹⁰³⁵, senza che sia necessario l'intervento di un'autorità giudiziaria nello Stato membro del prestatore di servizio¹⁰³⁶. Infatti, gli strumenti non dovrebbero operare nelle situazioni nazionali, ove è possibile – all'evidenza – ottemperare con misure nazionali dello stesso tipo.

Gli ordini dovrebbero essere rivolti a rappresentanti legali dei prestatori di servizi appositamente designati. Se un prestatore di servizi stabilito nell'Unione non ha designato

p. 23 ss.; R. JANSEN, *Explaining the methods for taking evidence abroad within the EU and some first observations on the proposal for the Evidence Regulation (recast)*, in *Nederlands Internationaal Privaatrecht*, 4, 2019, p. 753 ss.; J.H. JEPPESEN, G. NOJEIM, *Initial Observations on the European Commission's e-Evidence Proposals*, in www.cdt.org, 18 aprile 2018, disponibile al link: <https://cdt.org/insights/initial-observations-on-the-european-commissions-e-evidence-proposals/>; J.H. JEPPESEN, G. NOJEIM, *Assessing the European Commission's E-Evidence Proposals on Ten Human Rights Criteria*, in www.cdt.org, 18 aprile 2018, disponibile al link: <https://cdt.org/insights/assessing-the-e-evidence-directive-on-ten-human-rights-criteria/>; F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., p. 1 ss.; V. MITSILEGAS, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, cit., p. 263 ss.; L. MOXLEY, *EU Release of e-Evidence Proposal for Cross-Border Data Access*, in www.insideprivacy.com; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 57 ss.; O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss.; G. ROBINSON, *The European Commission's e-Evidence Proposal*, in *European Data Protection Law Review*, 3, 2018, p. 347 ss.; M. ROGALSKI, *The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 4, 2020, p. 333 ss.; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 1 ss.; F. RUGGIERI, *Novità. Il protocollo 16 alla Cedu in vigore dal 1° agosto 2018. La proposta per l'ordine europeo di conservazione o di produzione della prova digitale*, in *Cass. Pen.*, 7-8, 2018, p. 2660 ss.; A. SACHOULIDOU, *The key elements of the LIBE Committee's compromise proposal on e-evidence: a critical overview through a fundamental rights lens*, in *Global Affairs*, 16 novembre 2021, p. 1 ss., disponibile al link: <https://www.tandfonline.com/doi/full/10.1080/23340460.2021.1999173>; N.A. SMUHA, *Towards the EU Harmonization of Access to CrossBorder E-Evidence: Challenges for Fundamental Rights & Consistency*, in *European Criminal Law Review*, 1, 2018, 83 ss.; A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 46 ss.; V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 439 ss.; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 161 ss.

¹⁰³³ In tal senso, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2728.

¹⁰³⁴ Così, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1345.

¹⁰³⁵ Sul punto, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1284.

¹⁰³⁶ Così, D. CURLOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora)*, cit., p. 756.

un rappresentante legale, gli ordini possono essere indirizzati a un qualsiasi stabilimento del prestatore all'interno dell'Unione. Questa possibilità – si potrebbe definire residuale – consentirebbe di garantire l'efficacia del sistema qualora il prestatore di servizi non abbia nominato un apposito rappresentante ovvero qualora l'obbligo non sia ancora in vigore, non essendo trascorso il termine di recepimento della direttiva relativa alla nomina sui rappresentanti legali.

Inoltre, il Regolamento si applica anche se il prestatore di servizi non è stabilito o rappresentato nell'Unione europea, ma offre servizi sul territorio. La disposizione sarebbe desumibile dall'art. 3, par. 1 della proposta di Regolamento.

Per funzionare al meglio, gli ordini dovranno basarsi su un livello elevato di fiducia reciproca¹⁰³⁷ tra gli Stati membri e rispettare al contempo i diritti fondamentali e i principi riconosciuti in particolare dalla Carta dei diritti fondamentali dell'Unione europea¹⁰³⁸.

Da qui, la scelta da parte della Commissione di adottare la forma del Regolamento per disciplinare i nuovi strumenti basati su procedure *in rem*. Nel solco di un mutuo riconoscimento del tutto rinnovato, rivisitato, ripensato e probabilmente anche rafforzato per taluni aspetti¹⁰³⁹ (tanto da perdere in parte quelle caratteristiche proprie che negli anni aveva assunto e a cui tutti gli operatori si erano abituati, colorandosi di sfaccettature del tutto inedite ed a tratti disorientanti), il legislatore europeo ha pensato di creare strumenti che prevedano un contatto diretto tra l'autorità giudiziaria di uno Stato membro e il privato stabilito in un altro Stato membro, tant'è che vi è chi ritiene che gli strumenti siano basati, più che sul principio del mutuo riconoscimento, su un *tertium genus*, che richiede un elevato livello di fiducia reciproca¹⁰⁴⁰.

Si sarebbe al cospetto di uno strumento “di terzo tipo”, basato su una forma avanzata di fiducia reciproca. Ciò perché, in linea generale, per l'OEC e l'OEP non è previsto il riconoscimento del provvedimento emesso dall'autorità di emissione da parte dell'autorità di esecuzione, ma al tempo stesso – senza richiedere particolari formalità – il privato dovrà eseguire l'ordine ricevuto, secondo modalità sicure e affidabili e che consentano di stabilire l'autenticità e l'integrità del certificato.

La scelta del Regolamento trova la base giuridica nell'art. 82, par. 1, TFUE, il quale garantisce il riconoscimento reciproco delle decisioni con cui l'autorità giudiziaria dello Stato di emissione si rivolge ad una persona giuridica in un altro Stato membro e le impone obblighi, senza il previo intervento dell'autorità giudiziaria di tale altro Stato

¹⁰³⁷ Così, A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 48.

¹⁰³⁸ Tra tali diritti è possibile annoverare il diritto alla libertà e alla sicurezza, il rispetto della vita privata e familiare, la protezione dei dati personali, la libertà di impresa, il diritto di proprietà, il diritto a un ricorso effettivo e a un giudice imparziale, la presunzione di innocenza e i diritti della difesa, i principi della legalità e della proporzionalità e il diritto di non essere giudicato o punito due volte per lo stesso reato. Sul punto, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 432 ss.

¹⁰³⁹ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1341 ss., secondo cui va delineandosi «uno schema per certi versi inedito di mutuo riconoscimento, improntato – quantomeno in prima battuta – non sul tradizionale dialogo tra le autorità giudiziarie competenti dei diversi Paesi interessati dalla procedura di assistenza, bensì tra l'autorità giudiziaria del Paese emittente e la nuova figura del Rappresentante legale designato dai prestatori di servizi, interlocutore (non statale) specificamente deputato alla ricezione ed esecuzione degli ordini in questione».

¹⁰⁴⁰ Così, A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 49.

membro¹⁰⁴¹. Tuttavia, lo schema previsto per tali strumenti, in linea con quanto previsto dai principi dell'Unione europea, prevede l'eventuale intervento dell'autorità giudiziaria nello Stato di esecuzione ove necessario per far eseguire la decisione.

La preferenza per la forma del Regolamento rispetto alla direttiva sottende una valutazione a carattere globale e funzionale. Invero, secondo l'art. 288 TFUE, caratteristica di tale atto di diritto derivato è la portata generale, l'obbligatorietà in tutti i suoi elementi e la diretta applicabilità in ciascuno degli Stati membri.

Ciò lo rende particolarmente adatto a disciplinare la ricerca e formazione delle prove elettroniche transnazionali perché consente di ottenere norme uniformi, senza lasciare margini agli Stati per il recepimento¹⁰⁴², offrendo al tempo stesso chiarezza e maggiore certezza giuridica ed evitando la formazione di orientamenti ed interpretazioni contrastanti e divergenti negli Stati membri¹⁰⁴³.

¹⁰⁴¹ Cfr., *Relazione alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, Strasburgo, 17 aprile 2018, COM(2018) 225 final, p. 5 ss.

¹⁰⁴² Sulle problematiche relative al recepimento, è emblematico quanto accaduto per l'altra procedura *in rem* utile per la ricerca e formazione delle prove in materia penale: l'ordine europeo di indagine. Come si evince dalla *Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della direttiva 2014/41/UE*, cit., p. 16, vi sono difficoltà riguardo ad alcune disposizioni chiave della direttiva, quali i motivi di non riconoscimento o di non esecuzione. Inoltre, la Commissione continua a valutare il rispetto della direttiva da parte degli Stati membri e adotterà misure adeguate al fine di assicurare la conformità alle sue disposizioni in tutta l'Unione europea. Invero, nella comunicazione “*Diritto dell'Unione europea: risultati migliori attraverso una migliore applicazione*” (C/2016/8600), in GUUE C/18 del 19 gennaio 2017, la Commissione ha chiarito che esamina in via prioritaria i casi nei quali gli Stati membri hanno recepito in modo scorretto le direttive, compiendo una valutazione strutturata, sistematica ed efficace del recepimento e delle misure nazionali che attuano la normativa dell'UE, ed individuando le lacune e il recepimento scorretto. Giova ricordare che anche sul versante delle procedure *in personam*, come il mandato di arresto europeo, si sono verificate problematiche affini. Infatti, la disciplina italiana, prevista con l. 22 aprile 2005, n. 69, di recepimento della decisione quadro, è stata conformata alla decisione quadro 2002/584/GAI sul mandato di arresto europeo solo di recente, con le modifiche apportate con il d.lgs. 2 febbraio 2021, n. 10. Infatti, la disciplina previgente aveva reso obbligatori tutti i motivi di rifiuto. La riforma ha riequilibrato il sistema, prevedendo motivi di rifiuto obbligatori e facoltativi, così come previsto dalla decisione quadro 2002/584/GAI. Ad esempio, ha eliminato l'ipotesi di rifiuto obbligatorio della consegna relativa all'esistenza di prole di età inferiore ai tre anni. Sull'applicazione della disciplina così come di recente modificata, Cass., Sez. VI, 26 maggio 2021, n. 21336, in *Ced Cass.*, rv. 281509, secondo cui anche a seguito della modifica dell'art. 7 della legge 22 aprile 2005, n. 69, per effetto del d.lgs. 2 febbraio 2021, n. 10, il requisito della doppia punibilità costituisce presupposto indispensabile per potersi far luogo alla consegna, fermo restando che non è necessario che coincidano la qualificazione giuridica ed i singoli elementi costitutivi delle fattispecie incriminatrici previste dallo Stato richiedente e da quello richiesto. (In applicazione del principio, la Corte ha escluso la ricorrenza della doppia punibilità con riferimento a condotte di contrabbando inquadrabili negli artt. 292 e 294 del d.P.R. 23 gennaio 1973, n. 43, trattandosi di reati depenalizzati dall'art. 1, comma 1, del d.lgs. 15 gennaio 2016, n. 8); Cass., Sez. VI, 26 maggio 2021, n. 25333, in *Ced Cass.*, rv. 281533, secondo cui la pronuncia che disponga la consegna precedentemente negata con decisione definitiva non configura violazione del principio del “*ne bis in idem*” qualora sia intervenuta una modifica della normativa interna applicabile. (Fattispecie in tema di abrogazione, successiva al primo rifiuto di consegna, dell'art. 18, lett. p), legge n. 69 del 22 aprile 2005 ad opera del d.lgs. 2 febbraio 2021, n. 10, che ha eliminato l'ipotesi di rifiuto obbligatorio della consegna relativa all'esistenza di prole di età inferiore ai tre anni). In dottrina, D. CURLOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e “Vecchia Europa”: una normativa che non c'è (ancora)*, cit., p. 756.

¹⁰⁴³ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1340. V., inoltre, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 292, i quali, nell'osservare che la scelta del Regolamento eviti la formazione di declinazioni diverse nei vari sistemi, ritengono che ciò sia «una precisa riprova di quanto

In merito a tale scelta, la dottrina ha evidenziato alcuni profili problematici.

Per quanto attiene al primo, ci si è chiesti se l'art. 82, par. 1, TFUE abiliti l'Unione europea a prevedere strumenti che consentano il rapporto diretto tra autorità pubblica e privato. Secondo una prima prospettazione, la norma farebbe riferimento soltanto ad un rapporto diretto basato sul principio del mutuo riconoscimento tra autorità giudiziarie. Di conseguenza, non sarebbe possibile prevedere uno strumento che abiliti un'autorità di uno Stato membro a richiedere elementi elettronici direttamente ad un privato presente sul territorio di un altro Stato membro¹⁰⁴⁴.

Altri invece ritengono che il mutuo riconoscimento non sottenda necessariamente il rapporto tra autorità giudiziarie, ma possa operare anche prescindendo dall'interlocazione diretta tra autorità. Pertanto, sarebbe possibile una collaborazione diretta tra un'autorità giudiziaria straniera e un *service provider*¹⁰⁴⁵.

Ed invero, l'art. 82, par. 1, TFUE, dispone che possano essere adottate, secondo la procedura legislativa ordinaria, misure volte a definire norme e procedure per assicurare il riconoscimento in tutta l'Unione di qualsiasi tipo di sentenza ovvero decisione giudiziaria, non precisando la necessità di un contatto tra autorità giudiziarie.

Infatti, non sembrerebbe necessario che nella notifica e nell'esecuzione dell'ordine sia direttamente coinvolta un'autorità pubblica del Paese in cui ha sede il destinatario della decisione. Di conseguenza, un cittadino dell'Unione europea sarà esposto all'accesso ai dati da parte di un'autorità di un altro Stato membro in base alla normativa di quest'ultimo¹⁰⁴⁶.

Vi è poi chi ha posto l'attenzione sul principio di territorialità¹⁰⁴⁷. Si è detto che la scelta del Regolamento – in luogo di una direttiva – al fine di conseguire un'armonizzazione sia forzata nella parte in cui assegna agli Stati membri una inammissibile giurisdizione extraterritoriale che consente ad uno Stato richiedente di esigere da un privato stanziato in un altro Stato la collaborazione al fine di formare una prova elettronica¹⁰⁴⁸.

Tuttavia, vi è chi, *contra*, saluta con favore tale innovazione, perché un approccio territoriale alla giurisdizione – basato sull'ubicazione dei dati – non solo appare poco

l'Unione ormai si fidi talmente poco di come gli Stati membri sono soliti recepire gli atti eurounitari in materia processuale penale, da aver tentato in questo caso di bypassare alla radice ogni problema di attuazione interna, proponendo un atto *self-executing*». Dello stesso parere, anche, A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 47.

¹⁰⁴⁴ In tal senso, G. ROBINSON, *The European Commission's e-Evidence Proposal*, cit., p. 352; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 13.

¹⁰⁴⁵ Così, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 5 ss.

¹⁰⁴⁶ Cfr., *Parere del Comitato economico e sociale europeo sulla «Proposta di regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale» e sulla «Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali»*, cit., par. 3.6.

¹⁰⁴⁷ Sul tema, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 436, secondo i quali « En d'autres termes, l'instrument tend vers une extra-territorialité de l'État membre d'émission qui peut contraindre un fournisseur de service se situant sur le territoire d'un autre État à fournir des informations nécessaires à une enquête judiciaire ».

¹⁰⁴⁸ Così, F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., 1 ss.

pratico, ma è all'evidenza tecnologicamente superato¹⁰⁴⁹, dato il crescente uso del *cloud computing*¹⁰⁵⁰, destinato a cambiare radicalmente la società e ad imporre sullo scenario giuridico un nuovo modo di riflettere e pensare la materia penale.

Non va poi dimenticato l'approccio estremamente pratico dell'Unione europea: si vuole evitare che il classico sistema basato sul contatto tra autorità giudiziarie rischi di non portare a risultati apprezzabili o addirittura di non conseguire alcun risultato, se non al costo di sprecare ingenti forze per trovare i dati necessari, mediante l'uso anche di costosi strumenti di decrittazione, sempre che ciò sia possibile, attraverso perquisizioni e sequestri nei centri di conservazione dei dati¹⁰⁵¹.

Deve comunque considerarsi come tale approccio vada incontro ad un'opera di revisione globale delle discipline, di una vera e propria razionalizzazione – *rectius*, unificazione normativa – che probabilmente potrà compiere il Regolamento, con il quale potrebbero essere evitate le continue difficoltà applicative relative ai conflitti di obblighi giuridici che dovranno affrontare i fornitori di servizi, qualora i quadri giuridici che si troveranno ad applicare siano tra di loro contrastanti.

Vi è, infine, chi ha sollevato alcune perplessità circa la tecnica di redazione e la conseguente scelta della forma del Regolamento¹⁰⁵² che, purtuttavia, tradisce un approccio "misto", rinvenendosi a tratti norme che vincolerebbero gli Stati destinatari solo per i risultati da raggiungere, rimettendo alle singole legislazioni nazionali la scelta dei mezzi e delle forme necessarie per conseguire il risultato prescritto, come avviene per le direttive. Il Regolamento, nel caso della disciplina prevista per le sanzioni ed i rimedi, si atteggierebbe a direttiva e potrebbe creare qualche differenza tra i Paesi dell'Unione europea.

¹⁰⁴⁹ Pioniere nell'abbandono del principio di territorialità è stato il Belgio, il quale ha compiuto tale scelta dapprima grazie a delle pronunce giurisprudenziali e poi modificando il codice di procedura penale. In breve, si è scelto di estendere gli obblighi di cooperazione ai fornitori che offrono i propri servizi ai cittadini belgi, indipendentemente dall'ubicazione dei dati e dalla sede del servizio. Su tali scelte belghe, V. FRANSSEN, *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?*, in *European Data Protection Law Review*, 3, 2017, p. 534 ss.

¹⁰⁵⁰ In questo senso, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 168. Sul punto anche, J. DASKAL, *The Un-Territoriality of Data*, cit., p. 326 ss.; V. KRISHNAMURTHY, *Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters*, in *The Berkman Klein Center for Internet & Society Research Publication*, 3, 2016, p. 1 ss., disponibile al link: <https://dash.harvard.edu/bitstream/handle/1/28566279/SSRN-id2733350.pdf?sequence=1&isAllowed=y>.

¹⁰⁵¹ Sugli aspetti tecnici e giuridici relativi a tale problematica, K. LIGETI, G. ROBINSON, *Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?*, in AA.VV., *Vielfact des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag* (R. KENT, A. LEHNER eds.), Wien, 2018, p. 625 ss.

¹⁰⁵² Sul punto, v., O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 6. Cfr., anche, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2725, secondo la quale «non è di immediata comprensione perché, invece di prevedere delle modifiche al testo della Direttiva 41/2014 sull'OIE, con definizioni e disposizioni specifiche anche per la prova elettronica (così come è stato fatto, per esempio, per la raccolta delle prove in tempo reale), l'eurolegislatore abbia preferito un'alternativa senza dubbio più complessa, legata alla produzione di un diverso testo normativo, di natura regolamentare, che non sarà sempre applicabile in modo coerente rispetto alla direttiva OIE e, con essa, alle singole scelte degli Stati Membri».

L'arguto rilievo merita qualche riflessione che valuti globalmente e sistematicamente il modo di operare proprio dell'Unione europea attraverso gli atti di diritto derivato e come questo metodo abbia influenzato le scelte della Commissione.

Preliminarmente, si deve rammentare che, come più volte osservato dalla Corte di giustizia, l'identificazione dell'atto non va fatta semplicemente in base al *nomen iuris*, ma in considerazione dei suoi caratteri sostanziali; e ciò, in ragione delle conseguenze pratico-giuridiche di estrema rilevanza, come l'accertamento della legittimità e la definizione degli effetti obbligatori¹⁰⁵³.

La Corte di giustizia ritiene anche possibile che un Regolamento possa richiedere delle misure di attuazione nazionali. Queste non snaturano il Regolamento, il quale conserva la propria funzione nel sistema delle fonti¹⁰⁵⁴.

Sicuramente, è ipotizzabile che al Regolamento succederanno uno o più atti di esecuzione da parte degli Stati membri, in virtù di una disciplina non pienamente *self-executing* e che manifesta la necessità di determinare alcuni elementi fondamentali per la pratica attuazione¹⁰⁵⁵ ed è condivisibile la prospettazione e la conseguente preoccupazione di possibili differenze tra ordinamenti relativi a quegli elementi di intervento di adattamento nazionali necessari, dettati dalla natura aperta di alcune norme.

Tuttavia, va comunque fatto affidamento sull'attività di vigilanza della Commissione, che, in qualità di custode dei trattati, ha il dovere di monitorare l'operato degli Stati membri nell'attuazione della legislazione dell'Unione europea e di garantire la conformità della loro normativa e delle loro prassi a tale legislazione, sotto il controllo della Corte di giustizia dell'Unione europea¹⁰⁵⁶.

Una possibile facilitazione di tale operazione potrebbe essere la redazione di una relazione di valutazione sul funzionamento del Regolamento, da compiersi periodicamente, come già sta previsto per l'ordine europeo di indagine, all'art. 37 della

¹⁰⁵³ In dottrina, U. VILLANI, *Istituzioni di diritto dell'Unione europea*, cit., p. 310. La giurisprudenza dell'Unione europea è costante nel valorizzare il requisito della sostanza rispetto a quello della forma dell'atto. A tal fine, v., Corte di giustizia, sentenza 1° novembre 2009, causa C-370/07, *Commissione/Consiglio*, punto 42; Trib. UE, sentenza 2 marzo 2010, causa T-16/04, *Arcelor/Parlamento e Consiglio*, punto 94; Corte di giustizia, sentenza del 13 ottobre 2011, cause riunite C-463/10P e C-475/10P, *Deutsche Post e Germania/Commissione*, punti 36-44; Trib. UE, sentenza del 16 ottobre 2014, causa T-517/12, *Alro SA/Commissione europea*, punto 22; Corte di giustizia, Grande Sezione, sentenza del 20 febbraio 2018, causa C-16/16P, *Belgio/Commissione*, punto 31; Corte di giustizia, Grande Sezione, sentenza del 9 luglio 2020, causa C-575/18P, *Repubblica Ceca/Commissione*, punto 46; Corte di giustizia, sentenza del 25 febbraio 2021, causa C-689/19P, *VodafoneZiggo Group BV/Commissione europea*, punti 46 e 98.

¹⁰⁵⁴ Cfr., Corte di giustizia, sentenza 11 gennaio 2001, causa C-403/98, *Azienda Agricola Monte Arcosu*, punto 26, in cui ha chiarito che «se, in conseguenza della natura stessa dei regolamenti e della loro funzione nel sistema delle fonti del diritto comunitario [oggi dell'Unione], le disposizioni dei detti regolamenti producono, in genere, effetti immediati negli ordinamenti giuridici nazionali, senza che le autorità nazionali debbano adottare misure di attuazione, talune loro disposizioni possono tuttavia richiedere, per la loro applicazione, l'adozione di misure di esecuzione da parte degli Stati membri». In giurisprudenza, anche, Corte di giustizia, sentenza del 24 giugno 2004, causa C-278/02, *Herbert Handlbauer GmbH*, punto 26; Corte di giustizia, sentenza 7 luglio 2011, causa C-523/09, *Rakvere Piim AS e Maag Piimatööstus AS/Veterinaar-ja Toiduamet*, punto 18. In dottrina, U. VILLANI, *Istituzioni di diritto dell'Unione europea*, cit., p. 310 ss.

¹⁰⁵⁵ In tal senso, sia consentito il rinvio a A. GAUDIERI, *Opposizione al decreto di riconoscimento dell'ordine europeo di sequestro: scenari*, cit., p. 2034.

¹⁰⁵⁶ Cfr., art. 17, par. 1, TUE.

direttiva 2014/41/UE¹⁰⁵⁷ e che ha dimostrato di essere efficace, quantomeno perché consente di mettere ordine ed individuare problematiche specifiche e sistematiche.

Invero, anche la proposta di Regolamento relativo agli ordini europei di produzione e conservazione ha previsto all'art. 24 la redazione periodica di una relazione di valutazione sul funzionamento degli strumenti per la formazione delle prove elettroniche transnazionali, inclusiva di una valutazione relativa alla necessità di ampliarne l'ambito di applicazione e corredata da eventuali proposte legislative, che potrebbero aiutare la Commissione a vigilare sulla sua applicazione e a far emergere eventuali lacune nell'applicazione del Regolamento.

La scelta della forma regolamentare dovrebbe essere salutata con favore, perché consente un'effettiva uniformazione della disciplina su tutto il territorio dell'Unione europea e permette di superare sin da subito quegli elementi di frizione che si sarebbero potuti creare con l'adozione di una direttiva.

Del resto, la specificità delle procedure transfrontaliere sembrerebbe proprio suggerire la previsione di norme uniformi, senza lasciare margini di recepimento agli Stati membri. Dunque, la forma più appropriata per tale strumento di mutuo riconoscimento sembra essere il Regolamento, il quale consente, appunto, di imporre lo stesso obbligo in modo uniforme in tutta l'Unione europea.

È vero che per alcuni istituti rilevanti si rischia di avere una disciplina differente tra gli Stati, ma è anche vero che per tanti altri ciò è evitato proprio grazie all'adozione di questa forma in luogo della direttiva, che non pochi problemi ha creato con l'ordine europeo di indagine.

Ad oggi, non appare possibile prevedere con Regolamento l'indicazione di mezzi e forme, oltre che di obiettivi, per gli istituti relativi ai rimedi ed alle sanzioni, perché si rischia un'ingerenza eccessiva nello Stato membro, relativa alla giurisdizione penale. Ciò perché opererebbe una preclusione relativa a tale assetto, in base a quanto attualmente previsto dai trattati. Tuttavia, aperture in tal senso sarebbero possibili in un prossimo futuro, purché in controtendenza alle attuali spinte sovraniste.

Sul punto, per garantire uniformità e tendere alla nomofilachia sarebbe auspicabile la creazione di un giudice penale europeo, almeno per le ipotesi relative alle impugnazioni di determinati strumenti di cooperazione, soprattutto se si considera che è ormai operativo un organo giudiziario europeo: EPPO.

Ciò su cui bisognerebbe riflettere, se si vogliono individuare possibili problematiche che rischiano di sorgere a causa della scelta della forma regolamentare – superabili, in ogni caso, in un'ottica propositiva – è il difficile coordinamento tra due atti legislativi facenti parte dello stesso “pacchetto”.

Orbene, la Commissione da una parte ha proposto la creazione di due strumenti (gli ordini europei di produzione e conservazione) da disciplinare con un Regolamento; dall'altra vuole obbligare gli Stati membri ad armonizzare la disciplina relativa alla nomina sui rappresentanti legali ai fini dell'acquisizione delle prove nei procedimenti penali mediante una direttiva.

¹⁰⁵⁷ L'art. 37, direttiva 2014/41/UE stabilisce che «entro cinque anni dal 21 maggio 2014, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione della presente direttiva, sulla base di dati sia qualitativi sia quantitativi fra cui, in particolare, la valutazione del suo impatto sulla cooperazione in materia penale e sulla protezione delle persone, nonché l'esecuzione delle disposizioni riguardanti l'intercettazione delle telecomunicazioni alla luce degli sviluppi tecnici. Tale relazione è corredata, se necessario, di proposte di modifica della presente direttiva».

Sembrerebbe chiara la sussistenza di un rapporto funzionale tra la direttiva ed il Regolamento, perché in tanto potrebbe funzionare perfettamente il Regolamento, in quanto gli Stati abbiano provveduto a recepire la direttiva.

Bisognerebbe riflettere se questa tecnica non possa in qualche modo rallentare l'operatività degli strumenti e se non si debba richiedere agli Stati membri una seria, efficiente e celere attività di recepimento della direttiva, se non si ritenga idoneo o possibile o, più semplicemente, opportuno far confluire tutta o parte della disciplina sulla nomina dei rappresentanti legali nel Regolamento¹⁰⁵⁸.

In realtà, nell'adottare un approccio pragmatico, la scelta del Regolamento è proiettata al raggiungimento di scopi di non poca rilevanza rispetto allo scenario caratterizzato da elementi elettronici volatili e facilmente alterabili, trasferibili e cancellabili: evitare un *iter* procedurale per la formazione delle prove troppo lungo nonché predisporre un quadro giuridico chiaro ed uniforme, che permetta ai prestatori di servizi di conservare o produrre con celerità i dati alle autorità giudiziarie che ne fanno richiesta¹⁰⁵⁹.

5. La funzione e l'ambito di applicazione degli ordini europei di produzione e conservazione

Gli ordini previsti dalla proposta di Regolamento hanno due diverse funzioni. L'ordine europeo di conservazione (OEC) consiste nella decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro di conservare prove elettroniche in vista di una successiva richiesta di produzione; mentre l'ordine europeo di produzione (OEP) è la decisione vincolante di un'autorità di emissione di uno Stato membro che ingiunge a un prestatore di servizi che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro di produrre elementi elettronici aventi attitudine probatoria.

Sebbene il profilo definitorio dei due strumenti possa apparire approssimativo e generare perplessità interpretative ed applicative¹⁰⁶⁰, è possibile dedurre che l'ordine europeo di conservazione si atteggi a strumento di eventuale attivazione per l'esecuzione di attività prodromiche e preliminari a quelle relative alla produzione dei dati elettronici, ed è dunque finalizzato ad una successiva richiesta di produzione dei dati temporaneamente “congelati” con l'OEC. Il congelamento del dato ad oggetto dell'OEC – la c.d. conservazione – evita che esso sia cancellato ovvero modificato.

I provvedimenti, che ricorderebbero in qualche modo le *injunction* di origine anglosassone¹⁰⁶¹, devono essere emessi o convalidati da un'autorità giudiziaria di uno

¹⁰⁵⁸ Qualcosa di simile pure è stato prospettato dalla Commissione LIBE. Cfr., COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, 24 ottobre 2019, PE642.987v00-01, p. 146 ss.

¹⁰⁵⁹ Così, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1284; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1342.

¹⁰⁶⁰ Su tale profilo critico, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2729.

¹⁰⁶¹ In tal senso, F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., 1 ss.

Stato membro, ed inviati ad un prestatore di servizi operante sul territorio dell'Unione europea, o a un rappresentante legale da esso designato che si trova in uno Stato membro, per mezzo di moduli *standard* dedicati: il certificato di ordine europeo di conservazione (*European Preservation Order Certificate*, EPOC-PR) ed il certificato di ordine europeo di produzione (*European Production Order Certificate*, EPOC)¹⁰⁶².

Gli strumenti hanno ad oggetto unicamente elementi conoscitivi capaci di produrre informazioni già esistenti, ossia già in possesso e conservati dai prestatori di servizi al momento della ricezione dell'ordine, anche se criptati¹⁰⁶³. Non possono invece essere utilizzati per le intercettazioni in tempo reale dei dati informatici¹⁰⁶⁴. In tal caso andrebbe attivata la procedura prevista dall'ordine europeo di indagine qualora l'esecuzione debba avvenire in uno Stato membro, ovvero un altro strumento rogatorio.

E proprio in relazione al rapporto che avranno questi strumenti con l'ordine europeo di indagine, va da subito chiarito che l'OEC e l'OEP non sostituiscono l'ordine europeo di indagine ai fini dell'ottenimento di prove elettroniche, ma lo affiancano¹⁰⁶⁵. Infatti, le autorità nazionali competenti potranno continuare ad utilizzare gli strumenti già esistenti quando li ritengano più pertinenti e più appropriati¹⁰⁶⁶.

Ciò vuol dire che le autorità degli Stati membri saranno libere nella scelta dell'uno o dell'altro strumento, attivando la procedura che riterranno più idonea al caso concreto. Infatti, nel caso di una richiesta che prevederà l'esecuzione di più tipi di attività d'indagine, l'autorità giudiziaria potrà scegliere di utilizzare l'ordine europeo di indagine anche per la produzione di prove elettroniche da un altro Stato membro.

¹⁰⁶² La disciplina relativa ai certificati di ordine europeo di conservazione e di ordine europeo di produzione è prevista all'art. 8 della proposta di Regolamento. I moduli *standard* figurano negli allegati I e II del Regolamento proposto e hanno la funzione di indicare le informazioni necessarie per il destinatario. Il modello standardizzato consentirebbe di ridurre al minimo gli errori, identificare agevolmente i dati ed abbattere i costi di traduzione, escludendo dati sensibili o che possono compromettere la segretezza ed il buon esito delle indagini. In tal modo, si dovrebbe facilitare l'esecuzione degli ordini di produzione e di conservazione. È previsto anche un terzo modulo *standard*, contenuto nell'allegato III, da compilare ed inviare all'autorità di emissione qualora il destinatario dell'ordine non possa ottemperare all'obbligo indicato, ovvero non possa rispettare il termine specificato o non fornisca i dati in modo esaustivo. I moduli devono essere tradotti dall'autorità di emissione in una delle lingue ufficiali dell'Unione europea indicata dal prestatore di servizi; ove tale scelta non avvenga, è possibile tradurli in una delle lingue ufficiali dello Stato membro in cui risiede o è stabilito il rappresentante legale del prestatore di servizi. Sul punto, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 436; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 80.

¹⁰⁶³ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1345 ss.

¹⁰⁶⁴ Così, D. CURLOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora)*, cit., p. 756; M. DANIELE, *Intercettazioni ed indagini informatiche*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), cit., p. 491; F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., I ss. Cfr., anche, *considerando* n. 19, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹⁰⁶⁵ Cfr., *considerando* n. 61, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹⁰⁶⁶ In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 68.

Al contrario, qualora l'acquisizione della prova elettronica sia l'unico atto d'indagine transnazionale che l'autorità nazionale deve compiere, date le caratteristiche degli strumenti, appare tendenzialmente più efficiente utilizzare l'OEC e l'OEP¹⁰⁶⁷.

Tale circostanza potrebbe creare casi di sovrapposizioni tra i due strumenti, con conseguente "scollamento" applicativo¹⁰⁶⁸.

Inoltre, bisognerebbe chiedersi se sarà totalmente demandato alla discrezionalità di chi attiva il procedimento la scelta tra procedura per OEI piuttosto che per ordine europeo di produzione, ovvero se verranno individuati dai singoli Stati membri dei criteri da seguire, considerato che la proposta di Regolamento si limita a consentire alle autorità degli Stati membri di scegliere lo strumento più adatto al caso concreto.

Nella scelta dello strumento più opportuno, sarebbe indispensabile ispirarsi al principio di proporzionalità e di adeguatezza, in modo da procedere ad un bilanciamento degli interessi e dei diritti in gioco, riguardanti tanto i diritti dell'indagato, quanto quelli delle persone (fisiche o giuridiche) coinvolte dal compimento dell'atto richiesto¹⁰⁶⁹.

La procedura per la formazione dell'e-evidence è particolarmente semplice e snella, caratterizzata da pochi passaggi e dai tempi significativamente ridotti, perché, ai sensi dell'art. 9 della proposta di Regolamento, la consegna delle informazioni elettroniche deve avvenire in dieci giorni ovvero – in situazioni di emergenza – in sei ore, dimostrando di essere uno strumento particolarmente celere rispetto ai sistemi rogatoriali "classici" basati sul principio della mutua assistenza, con i quali è possibile ottenere le informazioni in circa dieci mesi, ovvero all'ordine europeo di indagine, con il quale è possibile ottenere un elemento avente attitudine probatoria in circa centoventi giorni¹⁰⁷⁰.

La decisione di creare due nuovi strumenti, da disciplinare in un unico atto legislativo con norme omogenee, è stata preceduta da una riflessione relativa ai possibili scenari futuri¹⁰⁷¹.

Le situazioni future prospettabili – e, dunque, analizzate – sono cinque. Nel primo scenario, si analizza l'attuale situazione, basata essenzialmente sulla *voluntary disclosure*

¹⁰⁶⁷ Così, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 69.

¹⁰⁶⁸ Per tale aspetto, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2729.

¹⁰⁶⁹ Così argomentando, a parità di efficacia, sarà da preferire sempre lo strumento che abbia conseguenze meno afflittive e riduttive dei diritti fondamentali. La proporzionalità-adequatezza impone di porre in bilanciamento, da un lato, le limitazioni di garanzie imposte ai singoli e, dall'altro, il valore del fine perseguito dall'autorità giudiziaria nell'esercizio della funzione, in ragione del particolare tipo di prova richiesta. Diversamente, la discrezionalità relativa all'attivazione di uno strumento piuttosto che dell'altro sembra celare dubbi relativi alla tutela dei diritti fondamentali della persona.

¹⁰⁷⁰ In tal senso, L. BUONO, *The genesis of European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, cit., p. 311; H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 436; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 80ss.; O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss.; A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 47; V. TONDI, *L'accesso transfrontaliero all'electronic evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 447.

¹⁰⁷¹ Cfr., Documento di lavoro dei servizi della Commissione – *Impact Assessment accompanying the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD(2018) 118.

e sulla discrezionalità degli *internet service provider* di produrre i dati elettronici. Innanzi a tale scenario, la situazione potrebbe solo peggiorare con l'aumentare delle richieste in un mondo fortemente digitalizzato.

Per risolvere le criticità, è dunque necessario agire scegliendo una delle successive quattro opzioni.

L'opzione A, a carattere non legislativo, prevede la formulazione di misure pratiche volte a migliorare le procedure di cooperazione giudiziaria e la cooperazione diretta tra le autorità pubbliche e i prestatori di servizi. In tal caso, la qualità delle richieste si innalzerebbe, ma permarranno i difetti strutturali dell'attuale sistema.

In uno scenario di tipo B, si è analizzato un primo intervento legislativo a carattere internazionale, affiancato all'indicazione di misure pratiche. Si tratterebbe di soluzioni internazionali a livello bilaterale o multilaterale combinate con le misure pratiche previste nell'opzione A. Siffatta scelta migliorerebbe il quadro relativo la formazione delle prove elettroniche transnazionali. Tuttavia, soffre di alcune incertezze, perché l'efficacia degli strumenti dipenderebbe in larga misura dagli Stati terzi.

L'opzione C combina le soluzioni a carattere internazionale con un ordine europeo di produzione e una misura per migliorare l'accesso alle banche dati che forniscono informazioni sugli abbonati sulla base di una ricerca, come il sistema WHOIS per i nomi di dominio. Tale scelta apporterebbe chiaramente un valore aggiunto rispetto alle precedenti opzioni e inoltre fornirebbe uno strumento agli Stati membri dell'Unione europea basato sul mutuo riconoscimento che consentirebbe la cooperazione diretta con i prestatori di servizi e che risponderebbe alla maggior parte delle problematiche individuate nel caso in cui un prestatore di servizi detenga i dati ricercati.

Infine, c'è un'ultima opzione – invero, non considerata dalla Commissione perché particolarmente incisiva – che prevede l'impiego di tutte le misure previste in tutti gli scenari e lo sviluppo di una misura legislativa sull'accesso diretto nelle situazioni in cui il coinvolgimento del prestatore di servizi non è necessario.

Pertanto, la Commissione ha ritenuto opportuno concentrarsi sulla creazione di due strumenti basati sullo scenario di tipo C, considerando che tale iniziativa possa aumentare l'efficacia e l'efficienza delle indagini e delle azioni penali, nel pieno rispetto della trasparenza e della responsabilità, sotto l'egida della tutela dei diritti fondamentali¹⁰⁷².

Infatti, tali strumenti consentono alle autorità nazionali di rivolgersi direttamente ai *service providers* che offrono servizi nello spazio di libertà, sicurezza e giustizia – anche se la sede centrale è posta in uno Stato terzo – per obbligare loro alla conservazione o alla produzione di elementi conoscitivi in formato elettronico¹⁰⁷³.

¹⁰⁷² Così, *Relazione* alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, COM(2018) 225 final, p. 9.

¹⁰⁷³ In tal senso, C. BRIÈRE, *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, cit., p. 501; O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 10; E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2728; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1343 ss.; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 282; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 10.

La soluzione prescelta tenterebbe di risolvere alcune criticità sviluppatesi nel tempo. Infatti, seppur con approcci diversi, alcuni Stati hanno adottato misure volte ad assicurare l'accesso alle informazioni digitali utili nell'ambito dei procedimenti penali, ampliando la competenza delle autorità giudiziarie nell'esecuzione di un atto d'indagine ovvero obbligando i *service provider* a designare un rappresentante legale sul proprio territorio¹⁰⁷⁴.

Ad esempio, in Italia si è sviluppato l'uso del captatore informatico – un *virus trojan* – inserito nei dispositivi al fine di procedere alla perquisizione *online*, ritenuto mezzo di ricerca della prova atipico¹⁰⁷⁵. Tuttavia, il *software* non garantirebbe secondo alcuni la genuinità del dato né la possibile alterazione di esso, oltre a costituire una pratica *borderline*, tendenzialmente sproporzionata e lesiva dei diritti fondamentali¹⁰⁷⁶.

Le problematiche relative alla frammentarietà delle legislazioni nazionali sul tema, le incertezze sull'obbligatorietà delle discipline nazionali nei confronti dei singoli prestatori di servizi stanziati sul territorio di altri Stati membri, la diversità e le divergenze dei regimi applicabili, l'aumento dei costi per le imprese, il ricorso a tecniche investigative non disciplinate nel dettaglio e di certo poco garantiste dei diritti fondamentali hanno spinto l'Unione europea a compiere questa scelta coraggiosa ma che la dottrina saluta «in modo alquanto positivo»¹⁰⁷⁷.

Gli entusiasmi sarebbero dovuti anche ad una valutazione – *prima facie*, opportunistica, ma che assolutamente non lo è – relativa all'assenza di una disciplina precisa laddove un'attività simile già si esegue per cortesia istituzionale o per mera collaborazione dei privati, che, tuttavia, forti di una disciplina assente, accentuano la propria discrezionalità indicando addirittura essi stessi i limiti o evitando comunque di produrre le informazioni richieste.

¹⁰⁷⁴ Ad esempio, nel 2017 la Germania ha adottato il *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* in base al quale obbliga i *service providers* a designare un soggetto sul territorio tedesco legittimato a ricevere le richieste di informazioni dalle autorità di contrasto.

¹⁰⁷⁵ In tal senso, M. DANIELE, *Le indagini informatiche contro il terrorismo. Bilanciamenti difficili e timori legislativi*, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali* (a cura di R. WENIN, G. FORNASARI), cit., p. 281.

¹⁰⁷⁶ Oltre che per le intercettazioni ambientali, il captatore informatico può essere utilizzato per sorvegliare ogni attività svolta attraverso un computer collegato ad internet. In tal caso si parla di *on-line surveillance* o di perquisizioni *on-line*. Se impiegato in tal modo, il captatore informatico diventa strumento “onnivoro”, capace di assorbire qualsiasi dato relativo anche a persone che non sono interessate dalle indagini e le cui informazioni, anche strettamente personali, transitano sul dispositivo informatico infettato. Sulla perquisizione *online*, non oggetto del presente lavoro, più ampiamente, F. CAPRIOLI, *Il “captatore informatico” come strumento di ricerca della prova in Italia*, in *Revista Brasileira de direito Processual Penal*, 2, 2017, p. 483 ss.; C. CONTI, M. TORRE, *Spionaggio digitale nell'ambito dei social network*, in AA.VV., *Le indagini atipiche* (a cura di A. SCALFATI), Torino, 2019, p. 535 ss.; D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *JusOnline*, 3, 2017, p. 382 ss.; K. LA REGINA, *Le indagini su dispositivi digitali*, in AA.VV., *Investigazioni digitali* (a cura di M. IASELLI), Milano, 2020, p. 64 ss.; S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.*, 7-8, 2010, p. 2855 ss.; L. PARLATO, voce *Perquisizioni on-line*, in *Enciclopedia del diritto, Annali*, X, 2017, p. 601 ss.; M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., p. 69 ss.; S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, cit., p. 291 ss.; A. TESTAGUZZA, *Digital forensics. Informatica giuridica e processo penale*, Padova, 2014, p. 90 ss.; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 436 ss.; M. TROGU, *Sorveglianza e “perquisizioni” online su materiale informatico*, in AA.VV., *Le indagini atipiche* (a cura di A. SCALFATI), Torino, 2014, p. 431 ss.

¹⁰⁷⁷ Per tale espressione, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 282.

Di fronte a tale situazione, del resto anche poco specchiata se la si vuole analizzare alla luce della tutela dei diritti fondamentali, non resta che guardare con favore ad un tentativo di disciplinare quella che ormai acquista i contorni di qualcosa che va al di là di una mera prassi, tentando oltretutto di assicurare il pieno rispetto dei diritti fondamentali coinvolti nella procedura.

In altre parole, se pure si deve ricorrere alla *voluntary disclosure* con tutte le implicazioni negative del caso, tanto vale disciplinare uno strumento, provando a trovare un equilibrio tra gli interessi in gioco e soluzioni che siano legalmente apprezzabili, in un mondo in continua mutazione e dove la digitalizzazione la farà sempre di più da padrona.

Dall'altra parte, è importante continuare nell'attività di vigilanza e tutela dei diritti fondamentali: è necessario valutare se effettivamente la disciplina allo studio tenga conto dei diritti fondamentali, in che modo li assicura e, nei meandri più oscuri della disciplina, se sia possibile individuare nuovi spazi sprovvisti di garanzie, privi di meccanismi preventivi, successivi e compensativi di eventuali lesioni dei diritti fondamentali.

Del resto, nel tracciare i principi della proposta di Regolamento, sia per l'OEC che per l'OEP, l'art. 1, par. 2, dispone l'obbligo di rispettare i diritti fondamentali e i principi giuridici sanciti dall'art. 6 TUE, compresi i diritti di difesa delle persone sottoposte al procedimento penale.

È nell'ottica pragmatica, di raggiungimento degli obiettivi, che opera l'Unione europea. Ed allora, notato che gli Stati membri non possono conseguire in misura sufficiente l'obiettivo di migliorare la protezione e l'ottenimento di prove elettroniche transfrontaliere, in applicazione del principio di sussidiarietà di cui all'art. 5 TUE, l'Unione europea ha deciso di adottare misure legislative che consentano, con proporzionalità, di tentare almeno di garantire una legale formazione dell'*e-evidence* transfrontaliera¹⁰⁷⁸.

La particolarità degli strumenti induce a chiedersi in quali casi e per quali procedimenti è possibile ordinare la produzione di elementi elettronici aventi attitudine probatoria nonché a chi inviare le relative richieste. A questi interrogativi dà risposta l'art. 3 della proposta di Regolamento.

Per un corretto approccio al tema, va preliminarmente indicata la struttura della proposta.

Al netto di una prima parte, composta dai c.d. *considerando*, il Regolamento si compone di 25 articoli, divisi in 5 Capi¹⁰⁷⁹.

Fanno parte del Capo 1 gli articoli da 1 a 3. Si tratta di alcune delle previsioni più importanti perché, ai fini della misura legislativa, danno alcune definizioni fondamentali, individuano l'oggetto dell'atto e determinano l'ambito di applicazione.

Il Capo 2 è la parte centrale dell'atto, perché indica la disciplina operativa degli ordini europei di produzione e di conservazione. Si tratta degli articoli da 4 a 12-ter, che individuano le autorità legittimate, le condizioni di emissione degli ordini, le modalità operative ed infine le attività di esecuzione.

¹⁰⁷⁸ Cfr., *considerando* n. 63, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹⁰⁷⁹ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1342; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 282.

Al Capo 3 sono descritte le sanzioni e la procedura di modifica con gli artt. 13 e 14. Si tratta di norme che hanno lo scopo di assicurare l'effettività al sistema di circolazione probatoria diretta¹⁰⁸⁰.

Dall'art. 15 all'art. 18, contenuti nel Capo 4, sono individuati i rimedi giurisdizionali, posti a necessaria e doverosa protezione del diritto di difesa¹⁰⁸¹ ed al fine di garantire un controllo effettivo sul corretto bilanciamento di tutti gli interessi posti in gioco.

Conclude il Regolamento il Capo 5, con alcune disposizioni finali relative alla lingua da utilizzare per la compilazione dei certificati degli ordini di conservazione e di produzione e le relazioni con altri strumenti, accordi e modalità.

Orbene, gli strumenti possono essere utilizzati solo per situazioni "transfrontaliere". Per cui un ordine vincolante può essere emesso solo per chiedere di conservare o produrre dati che sono conservati da un prestatore di servizi situato in un altro ordinamento, non potendo essere emesso per questioni meramente interne, ove è possibile avvalersi di misure nazionali¹⁰⁸². Ciò perché gli strumenti europei non devono limitare i poteri già conferiti dal diritto nazionale alle autorità nazionali competenti finalizzati a obbligare i prestatori di servizi stabiliti o rappresentati nel proprio territorio.

Tali misure possono essere utilizzate solo per procedimenti penali e per l'esecuzione di misure di sicurezza privative della libertà o di pene detentive che non sono state rese in contumacia in caso di latitanza o del condannato¹⁰⁸³. Per quanto riguarda gli enti da reato, si dispone che gli ordini possano essere emessi anche per procedimenti relativi a reati per cui una persona giuridica può essere considerata responsabile o punibile nello Stato di emissione¹⁰⁸⁴.

Appare chiaro che gli ordini europei di conservazione e produzione debbano essere emessi solo nell'ambito di specifici procedimenti penali nei confronti di specifici autori, noti ovvero ignoti, di un fatto-reato già commesso, purché lo strumento appaia necessario e proporzionato al singolo caso concreto¹⁰⁸⁵. Inoltre, simile previsione garantisce l'applicazione dei diritti procedurali applicabili nei procedimenti penali.

¹⁰⁸⁰ In tal senso, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 287.

¹⁰⁸¹ Così, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2727.

¹⁰⁸² Così, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 438; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1344; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 68.

¹⁰⁸³ Per quanto riguarda l'estensione dell'ambito di applicazione ai condannati latitanti, la Repubblica Ceca, la Finlandia, la Lettonia e la Germania hanno formulato una riserva. Sul punto, anche, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1344, secondo cui «tali strumenti possono essere adottati solo ove in relazione ad uno specifico reato già commesso sia avviato un apposito procedimento penale, nei confronti di autori noti o ancora ignoti. Proprio tale nesso con un'indagine particolare distingue, a ben vedere, gli ordini in esame dalle misure preventive e dagli obblighi di conservazione dei dati stabiliti dalla legge, assicurando altresì l'applicazione dei diritti e delle garanzie contemplati per i procedimenti penali». V., inoltre, A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, cit., p. 48.

¹⁰⁸⁴ Cfr., art. 3, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. Sul punto, anche, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 171.

¹⁰⁸⁵ Cfr., considerando n. 24, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. Cfr., inoltre,

Sembra possibile, dunque, che gli ordini siano emessi sia nella fase delle indagini preliminari sia nella fase processuale¹⁰⁸⁶, sino alla chiusura con sentenza o altra decisione¹⁰⁸⁷.

Per alcuni, sembrerebbe esclusa la fase esecutiva, non ricompresa solitamente nella fase processuale intesa in senso stretto¹⁰⁸⁸. Altri ritengono che l'OEC e l'OEP possano essere emessi anche in caso dell'esecuzione della sentenza penale di condanna prevista all'art. 656 c.p.p. o di una misura di sicurezza detentiva definitiva quando il soggetto si sia sottratto alla giustizia, purché non siano stati pronunciati in contumacia¹⁰⁸⁹.

Inoltre, bisognerebbe riflettere sul possibile rischio di limitazione – in astratto – dell'operatività dell'integrazione probatoria *ex officio* prevista all'art. 666, comma 5, c.p.p., sebbene, a causa del decorso del tempo, vi sia il pericolo che i dati possano già stati cancellati o alterati e, dunque, non siano più recuperabili presso i singoli prestatori di servizi.

Da quanto indicato dall'art. 3 della proposta di Regolamento, l'ambito di applicazione degli strumenti appare più limitato rispetto all'ordine europeo di indagine, laddove l'art. 4, direttiva 2014/41/UE, estende l'uso dell'ordine europeo di indagine anche nel quadro di un procedimento avviato dalle autorità amministrative in relazione a fatti punibili in base al diritto nazionale dello Stato di emissione in quanto violazioni di norme giuridiche, quando la decisione può dar luogo a un procedimento davanti a un organo giurisdizionale competente, segnatamente, in materia penale¹⁰⁹⁰.

In tal senso, sarebbe da escludere un possibile ricorso agli ordini di conservazione e produzione per le attività di monitoraggio preventivo di eventuali attività illecite che non siano iscritte nel registro delle notizie di reato di cui all'art. 335 c.p.p.¹⁰⁹¹

Per quanto riguarda la tipologia di dato richiedibile, che funge da ulteriore requisito per l'uso dell'OEP e dell'OEC, il combinato disposto dall'art. 3, par. 3 e dall'art. 2, punto 3) della proposta di Regolamento, chiarisce che gli ordini possono essere emessi solo per i dati riguardanti: i servizi di comunicazione elettronica come definiti dall'art. 2, punto 4)¹⁰⁹², direttiva 2018/1972/UE che istituisce il codice europeo delle comunicazioni

R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 75.

¹⁰⁸⁶ Sul punto, A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 13.

¹⁰⁸⁷ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1344.

¹⁰⁸⁸ Così, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 12.

¹⁰⁸⁹ In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 75.

¹⁰⁹⁰ In ogni caso, come chiarito al considerando n. 25, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, il Regolamento non pregiudica i poteri d'indagine delle autorità nei procedimenti civili o amministrativi, anche qualora tali procedimenti possano comportare sanzioni.

¹⁰⁹¹ In questi termini, F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., 1 ss.

¹⁰⁹² Si tratta dei i servizi forniti di norma a pagamento su reti di comunicazioni elettroniche, che comprendono, con l'eccezione dei servizi che forniscono contenuti trasmessi utilizzando reti e servizi di comunicazione elettronica o che esercitano un controllo editoriale su tali contenuti, i tipi di servizi seguenti: servizio di accesso a internet quale definito all'art. 2, secondo paragrafo, punto 2), del Regolamento (UE) 2015/2120 (ossia, un servizio di comunicazione elettronica a disposizione del pubblico che fornisce accesso a Internet, ovvero connettività a praticamente tutti i punti finali di Internet, a prescindere dalla tecnologia

elettroniche¹⁰⁹³; i servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la privacy o proxy¹⁰⁹⁴; gli altri servizi della società di informazione prestati normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi¹⁰⁹⁵ che offrono la possibilità per gli utenti di comunicare fra di loro oppure la possibilità di trattare o memorizzare dati per conto degli utenti ai quali è prestato il servizio.

Vi sarebbe da chiedersi se il continuo rinvio ad altre fonti non renda particolarmente complesso individuare i servizi a cui si applica il Regolamento e, di conseguenza, non renda difficile per gli operatori comprendere con chiarezza qual è l'effettivo campo di operatività.

Gli ordini europei di conservazione e di produzione vanno indirizzati ai prestatori di servizi che rientrano in particolari categorie.

Generalmente, si tratta di prestatori di servizi di comunicazione elettronica, della società dell'informazione come social network e mercati online, di nomi di dominio Internet e di numerazione IP attivi nell'Unione europea¹⁰⁹⁶.

di rete e dalle apparecchiature terminali utilizzate); servizio di comunicazione interpersonale; servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali come i servizi di trasmissione utilizzati per la fornitura di servizi da macchina a macchina e per la diffusione circolare radiotelevisiva.

¹⁰⁹³ Direttiva 2018/1972/UE del Parlamento europeo e del Consiglio che istituisce il codice europeo delle comunicazioni elettroniche, in GUUE L-321, del 17 dicembre 2018. In Italia la direttiva è stata recepita con d.lgs. 8 novembre 2021, n. 207, in GU n. 292 del 9 dicembre 2021.

¹⁰⁹⁴ Va considerato che i prestatori di servizi come i registrar di nomi di dominio e i registri e i prestatori di servizi per la privacy o proxy o i registri regionali di internet (Regional Internet Registry, RIR) per gli indirizzi del protocollo internet (IP) sono particolarmente rilevanti quando occorre identificare soggetti dietro siti web dannosi o compromessi ovvero per i procedimenti penali, in quanto permettono di identificare persone o entità dietro un sito web usato per scopi criminali o le vittime dell'attività criminale qualora un sito web compromesso sia stato piratato da criminali. Cfr. *considerando* n. 18, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹⁰⁹⁵ Il rinvio è all'art. 1, par. 1, lett. b), direttiva 2015/1535/UE del Parlamento e del Consiglio che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, in GUUE L-241, del 17 settembre 2015.

¹⁰⁹⁶ Così, C. BRIÈRE, *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, cit., p. 499; O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 10; H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 429 ss.; E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2728, secondo la quale «l'individuazione del destinatario dell'EPOC è un'attività fondamentale per la legittima applicazione degli strumenti in analisi e per la loro effettiva efficacia pratica»; V. FRASSEN, *The European Commission's e-Evidence Proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?*, cit., p. 1 ss.; O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss.; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 7; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 172.

Più nello specifico, ai sensi dell'art. 2, par. 2, proposta di Regolamento, per prestatore di servizi si intende la persona fisica o giuridica che fornisce una o più categorie di servizi, così come individuate dal Regolamento e poc'anzi esposte¹⁰⁹⁷.

Andrebbero esclusi, secondo quanto indicato dal Regolamento stesso, i prestatori che offrono servizi finanziari quali l'attività bancaria, il credito, l'assicurazione e la riassicurazione, le pensioni professionali o individuali, i titoli, gli investimenti, i fondi, i servizi di pagamento e quelli di consulenza nel settore degli investimenti¹⁰⁹⁸.

Invero, in armonia con quanto indicato anche dalla Convenzione sulla criminalità informatica, i prestatori di servizi ritenuti più adeguati a rispondere alle esigenze di tutela della collettività e, dunque, più idonei alla produzione di dati utili per un processo penale sono coloro che si occupano di comunicazione elettronica e coloro che facilitano l'interazione tra utenti come, ad esempio, chi si occupa di comunicazioni interpersonali basati sul sistema Voice over IP (VoIP), la messaggistica istantanea e i servizi di posta elettronica. Come pure, il Regolamento sembrerebbe applicabile ai prestatori di servizi che offrono agli utenti la possibilità di comunicare tra loro ovvero offrono servizi per il trattamento o la memorizzazione dei dati per loro conto. Ulteriori soggetti destinatari degli ordini dovrebbero essere anche coloro che offrono servizi relativi ai mercati online, i servizi di hosting e di *cloud computing*, nonché piattaforme online di gioco e di gioco d'azzardo¹⁰⁹⁹.

Allora, appare evidente che, nel rispetto del principio di proporzionalità, l'Unione europea intenda escludere tra i destinatari degli ordini di produzione e conservazione i prestatori di servizi che consentono ai propri utenti di comunicare solamente con il prestatore di servizi ovvero che non offrono la possibilità di trattare o conservare dati, esentando dalla produzione e conservazione dei dati, tra l'altro, anche i *service provider* il cui nucleo imprenditoriale non consista nel trattamento o nella conservazione dei dati, come ad esempio i servizi giuridici, architettonici, ingegneristici e contabili forniti online a distanza¹¹⁰⁰. Si tratterebbe di servizi per i quali la conservazione di dati non è la caratteristica principale, bensì un elemento puramente accessorio.

Una simile scelta sembra in linea con il livello di tutela dei diritti fondamentali garantiti nell'Unione europea, perché un siffatto sistema riuscirebbe a tutelare i dati ultrasensibili detenuti da talune categorie professionali, neutralizzando in qualche modo il pericolo per la segretezza delle informazioni relative ad una persona più attinenti alla

¹⁰⁹⁷ Tuttavia, vi è da dire che Finlandia, Lettonia e Lussemburgo hanno formulato una riserva, in quanto le autorità pubbliche non dovrebbero essere tenute a rispettare un ordine europeo di produzione o di conservazione (Finlandia). Sembrerebbe che la definizione sia tuttora troppo vaga e giuridicamente incerta (Lussemburgo) e sarebbe necessario esaminare ulteriormente la definizione, soprattutto in relazione alla proposta di direttiva che stabilisce norme armonizzate sulla nomina dei rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (Lettonia).

¹⁰⁹⁸ Il riferimento è all'art. 2, par. 2, lettera b), direttiva 2006/123/CE, del Parlamento e del Consiglio, relativa ai servizi nel mercato interno, del 12 dicembre 2006, in GUUE L-376, del 27 dicembre 2006, attuata in Italia con d.lgs. 26 marzo 2010, n. 59, in GU n. 75 del 23 aprile 2010.

¹⁰⁹⁹ Cfr., *considerando* n. 16, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. In dottrina, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 434.

¹¹⁰⁰ Sul punto, anche, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 10 ss. V., inoltre, *considerando* n. 16, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

sfera intima e personale e il cui disvelamento lederebbe la parte più profonda della dignità della persona umana.

Come già chiarito, il *service provider* può essere destinatario di un OEC o un OEP anche se ha la propria sede centrale in un Paese terzo¹¹⁰¹, purché offra i propri servizi sul territorio dell'Unione europea. In tal caso, gli ordini dovrebbero essere emessi solo per i dati relativi ai servizi offerti sul territorio dell'Unione.

Questa disciplina – invero, basata su scelte di principio del tutto simili a quelle operate negli Stati Uniti d'America con il *Cloud Act*¹¹⁰² – risentirebbe di una situazione di fatto particolare, frutto del progresso tecnologico e, di conseguenza, di una società che muta, cambia volto, aggiunge nuove sfaccettature a quelle già esistenti, perdendone altre al contempo. Infatti, così disponendo, si terrebbe conto di una circostanza ormai non poco sporadica e destinata a diventare una costante. Spesso, i dati non sono più conservati nel dispositivo dell'utente ma vengono indirizzati su un'infrastruttura *cloud*, che consente in linea di massima l'accesso da qualsiasi luogo e con qualsiasi dispositivo, mediante un sistema di chiavi d'accesso. I prestatori di servizi non hanno bisogno di essere stabiliti o avere *server* in ogni giurisdizione ma ricorrono piuttosto a un'amministrazione centralizzata e a sistemi decentrati per conservare i dati e fornire i servizi¹¹⁰³.

Uno sviluppo tecnologico di siffatta natura non poteva non essere considerato dal legislatore europeo, il quale ha tenuto conto dei servizi *cloud* e di altri servizi di *hosting* che forniscono una vasta gamma di risorse informatiche, quali reti, server o altre infrastrutture, mezzi di conservazione, app e servizi che permettono di conservare dati a diversi scopi, senza tralasciare l'ampio mondo dei mercati digitali che consentono ai consumatori ed imprese di concludere operazioni tramite contratti di vendita o di servizi *online*¹¹⁰⁴.

Proprio da tale assunto, si comprende l'approccio pragmatico, volto ad ampliare il campo di applicazione territoriale. Infatti, un'area di operatività limitata alla sola zona dell'Unione europea non consentirebbe di raggiungere gli obiettivi perseguiti dai nuovi strumenti.

Tuttavia, non è vero il contrario. Se il prestatore di servizi è stabilito nell'Unione europea, i servizi offerti esclusivamente al di fuori dell'Unione europea non rientrano nell'ambito di applicazione del Regolamento¹¹⁰⁵. Non vi sarebbe in tal caso alcun interesse concreto, legalmente apprezzabile, da parte dei singoli Stati ad ottenere

¹¹⁰¹ Così, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1343 ss.; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 282.

¹¹⁰² Per tale osservazione, R. BISMUTH, *Le Cloud Act face au projet européenne e-evidence: confrontation ou coopération?*, in *Revue de droit international privé*, 3, 2019, p. 685.

¹¹⁰³ Così facendo, si ottimizza il bilanciamento del carico e si riducono i tempi di risposta alle richieste di dati degli utenti. Le reti di diffusione di contenuti (CDN) sono generalmente usate per accelerare la fornitura di contenuti copiando i contenuti in più *server* diffusi in tutto il mondo. Le imprese possono così fornire i contenuti dal server più vicino all'utente o in grado di inoltrare la comunicazione attraverso una rete meno congestionata.

¹¹⁰⁴ Si pensi ad Amazon, probabilmente il più grande e più conosciuto mercato *online*. Le operazioni sono effettuate o sul sito web del mercato online o sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato *online*. È in questi mercati o nei mercati neri del *dark web* che generalmente si annidano le prove elettroniche necessarie nel corso di procedimenti penali.

¹¹⁰⁵ Cfr., considerando n. 26, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

informazioni relative ad attività extra-UE. Anche tale aspetto sarebbe influenzato dal principio di proporzionalità e dal principio di sovranità.

La disciplina sembra assicurare un trattamento paritario tra tutti i prestatori di servizi che operano nel mercato europeo, evitando, inoltre, che si venga a creare uno “spazio grigio” di elusione della disciplina, che consentirebbe ai criminali di poter operare in contesti non raggiunti dal Regolamento sugli ordini europei di produzione e conservazione.

In altre parole, ancora una volta con un approccio estremamente pragmatico, l’Unione europea ha voluto che tutti gli operatori che offrono i servizi sul territorio europeo siano obbligati a rispettare il Regolamento, per evitare che in qualche modo i criminali possano operare “sottotraccia”, senza essere scoperti, in territori virtuali inaccessibili dalla nuova disciplina.

Di conseguenza, l’applicazione del Regolamento si sgancerebbe dal principio del luogo effettivo in cui si trova lo stabilimento del prestatore o la struttura per il trattamento o la conservazione dei dati¹¹⁰⁶.

Orbene, bisogna compiere uno sforzo ermeneutico per comprendere cosa si intende per *service provider* che offre i propri servizi sul territorio dell’Unione europea.

Secondo l’art. 2 della proposta di Regolamento, offrire servizi nell’Unione significa consentire alle persone fisiche o giuridiche in uno o più Stati membri di usare i servizi, così come indicati, ovvero avere un collegamento sostanziale basato su specifici criteri di fatto con lo Stato membro o gli Stati membri.

La formulazione appare ombrosa, a tratti oscura, degna dei migliori *arcana juris*. L’assenza di chiarezza e precisione lascia spazio a fulgide spiegazioni prestate dai *considerando*, che – fortunatamente – provano a diradare le tempestose nubi dell’incertezza poste innanzi gli occhi dell’interprete.

E come Dante, smarritosi nella selva oscura, trovò soccorso in Virgilio, colui che successivamente gli farà da Cicerone in due dei tre regni dell’Oltretomba, così l’interprete del Regolamento dovrà saldamente ancorarsi al principio di proporzionalità ed a quanto indicato dai *considerando* per dissipare almeno parte dei propri dubbi, individuando i “criteri di determinazione”.

Secondo un primo criterio di determinazione, per determinare se un *service provider* offre i propri servizi nell’Unione le autorità devono verificare se il prestatore consente alle persone fisiche o giuridiche di uno o più Stati membri di usufruire dei suoi servizi. Non costituirebbe una condizione sufficiente per l’applicazione del Regolamento la semplice accessibilità del servizio¹¹⁰⁷, come ad esempio l’accessibilità del sito web del prestatore di servizi o di un intermediario o di un indirizzo di posta elettronica e di altri dati di contatto.

Il criterio di determinazione – alternativo e successivo al primo – sarebbe il collegamento sostanziale con uno Stato membro, che costituirebbe un nesso sufficiente tra il prestatore di servizi ed il territorio in cui i servizi sono offerti.

¹¹⁰⁶ Cfr., *considerando* n. 17, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹⁰⁷ Cfr., *considerando* n. 27, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. V., in dottrina, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1344 ss.

In tal caso, si dovrebbe valutare il legame effettivo tra il prestatore di servizi ed il territorio in cui i servizi sono offerti¹¹⁰⁸.

Il legislatore europeo sembra aver individuato tre “criteri di collegamento sostanziale”, l’uno successivo all’altro. Secondo un primo collegamento sostanziale, il prestatore di servizi deve avere uno stabilimento in uno o più Stati membri¹¹⁰⁹. In altre parole, il *service provider* deve esercitare effettivamente un’attività economica a tempo indeterminato con un’infrastruttura stabile a partire dalla quale viene svolta l’attività di prestazione di servizi o viene gestita l’attività. Il dato si ricava dall’art. 2, numero 5) della proposta di Regolamento.

In assenza di uno stabilimento nell’Unione europea, il criterio del collegamento sostanziale deve essere valutato sulla base di specifici criteri di fatto, come un numero significativo di utenti in uno o più Stati membri, o dell’orientamento sostanziale delle attività verso uno o più Stati membri¹¹¹⁰.

La *ratio* di tali scelte starebbe nella volontà del legislatore di creare in capo ai fornitori di servizi obblighi di legge ispirati ai concetti di sicurezza, di autorità nonché di libertà, nella stessa area geografica ove questi traggono profitto, a parità di condizioni tra i fornitori stessi¹¹¹¹.

Ci sarebbe da chiedersi se, per rispondere ad una richiesta di assistenza giudiziaria, possano emettersi degli ordini europei di produzione e conservazione. Nell’emendare la proposta, nell’orientamento generale, il Consiglio ha ritenuto opportuno precisare che non

¹¹⁰⁸ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1344 ss.

¹¹⁰⁹ Cfr., *considerando* n. 28, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹¹⁰ Cfr., *considerando* n. 28, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale, secondo cui l’orientamento delle attività verso uno o più Stati membri può essere determinato sulla base di tutte le circostanze pertinenti, tra cui l’uso di una lingua o di una moneta generalmente usata in uno Stato membro, o la possibilità di accedere a prodotti o servizi. Potrebbe anche desumersi dalla disponibilità di una app nell’apposito negozio online (“app store”) nazionale, dalla fornitura di pubblicità a livello locale o nella lingua usata in uno Stato membro, dal fatto che sono usate informazioni provenienti da persone presenti negli Stati membri nel corso delle attività o dalla gestione dei rapporti con la clientela, ad esempio la fornitura dell’assistenza alla clientela nella lingua generalmente usata in uno Stato membro. Il criterio del collegamento sostanziale dovrebbe inoltre considerarsi soddisfatto qualora il prestatore di servizi diriga le sue attività verso uno o più Stati membri, come previsto all’articolo 17, par. 1, lettera c), del Regolamento (UE) 1215/2012 concernente la competenza giurisdizionale, il riconoscimento e l’esecuzione delle decisioni in materia civile e commerciale. Tuttavia, la fornitura del servizio al fine del mero rispetto del divieto di discriminazione imposto dal Regolamento (UE) 2018/302, recante misure volte a impedire i blocchi geografici ingiustificati e altre forme di discriminazione basate sulla nazionalità, sul luogo di residenza o sul luogo di stabilimento dei clienti nell’ambito del mercato interno, non può di per sé considerarsi direzione o orientamento delle attività verso un dato territorio all’interno dell’Unione europea. In dottrina, C. BRIÈRE, *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, cit., p. 500 ss.; O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 11; E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2728; V. TONDI, *L’accesso transfrontaliero all’evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 446.

¹¹¹¹ Così, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 172.

si dovrebbe ricorrere a tali strumenti per fornire assistenza giudiziaria a un altro Stato membro o a un Paese terzo¹¹¹².

Del resto, nell'ottica di una maggior efficienza degli strumenti di cooperazione giudiziaria, sembrerebbe più confacente agli obiettivi che la richiesta di assistenza giudiziaria sia rivolta direttamente allo Stato membro o al Paese terzo che può fornire assistenza giuridica secondo il proprio diritto nazionale, eccetto nell'ipotesi in cui l'autorità di emissione abbia già ottenuto prove elettroniche a norma del Regolamento per propri procedimenti penali e tali prove siano in seguito oggetto di trasferimento o trasmissione. In tal caso si applicherebbe il principio di specialità¹¹¹³.

In conclusione, alla luce del principio di necessità e proporzionalità, che irradia l'intera proposta di Regolamento, sembra intravedersi l'applicazione del principio di gradualità: la disciplina è più stringente all'aumentare del grado di potenziale lesività dei diritti fondamentali.

6. L'ordine europeo di conservazione

L'ordine europeo di conservazione (OEC), ai sensi dell'art. 2, n. 2) della proposta di Regolamento, consiste in una decisione vincolante, oggetto di un provvedimento di un'autorità di emissione di uno Stato membro che ingiunge di conservare prove elettroniche in vista di una successiva richiesta di produzione a un prestatore di servizi che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro¹¹¹⁴.

Si tratta di uno strumento meno afflittivo rispetto all'ordine europeo di produzione¹¹¹⁵. Il provvedimento è volto alla neutralizzazione del pericolo di rimozione, cancellazione o modifica dei dati, a causa del decorso del tempo o dell'intervento umano, mediante la tecnica del "congelamento"¹¹¹⁶, in vista di una successiva richiesta di produzione dei

¹¹¹² In tal senso, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 171.

¹¹¹³ Cfr., *considerando* n. 24-bis e art. 3, par. 1-bis, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. Più specificamente, secondo il principio di specialità previsto all'art. 12-ter della proposta di Regolamento, le prove elettroniche non sono utilizzate ai fini di procedimenti diversi da quelli per i quali sono state ottenute conformemente alle disposizioni del Regolamento, tranne ai fini dei procedimenti per i quali avrebbe potuto essere rilasciato un ordine di produzione europea conformemente all'articolo 5, paragrafi 3 e 4 ovvero al fine di evitare una minaccia grave e immediata per la pubblica sicurezza dello Stato di emissione o i suoi interessi fondamentali. Inoltre, le prove elettroniche ottenute a norma del Regolamento possono essere trasmesse a un altro Stato membro, a un Paese terzo o a un'organizzazione internazionale unicamente ai fini dei procedimenti per i quali avrebbe potuto essere rilasciato un ordine di produzione europea conformemente all'articolo 5, paragrafi 3 e 4 ovvero al fine di evitare una minaccia grave e immediata per la pubblica sicurezza di tale Stato membro o i suoi interessi fondamentali.

Per il trasferimento ad un Paese terzo e ad una organizzazione internazionale vanno valutate anche le condizioni di cui al capo V della direttiva (UE) 2016/680.

¹¹¹⁴ Cfr., E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 283; V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 443.

¹¹¹⁵ R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1343.

¹¹¹⁶ Parla di "congelamento" dei dati in situazioni in cui potrebbe occorrere più tempo per chiedere od ottenere la produzione dei dati stessi, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel*

medesimi attraverso i canali tradizionali di assistenza rogatoria, o attraverso un ordine europeo di indagine ovvero un ordine europeo di produzione.

Si sarebbe in presenza di uno strumento che vuole tutelare l'esigenza di dispersione o compromissione della genuinità del dato elettronico avente attitudine probatoria.

L'OEC è un atto prodromico e preliminare alla eventuale e successiva attività di apprensione e trasferimento del prodotto del congelamento nello Stato di emissione che ha richiesto il dato per uno specifico procedimento penale.

Il procedimento si divide in due fasi. Una prima fase, detta di emissione, è dedicata alla formazione del provvedimento nonché alla compilazione e trasmissione del certificato di ordine europeo di conservazione (EPOC-PR). Pertanto, ha inizio con la valutazione delle condizioni per l'emissione dell'OEC e si conclude con la trasmissione dell'EPOC-PR al privato o con un eventuale provvedimento che non convalida l'OEC. Protagonisti di questa fase sono l'autorità di emissione e l'autorità di convalida. L'intervento di quest'ultima è eventuale perché previsto solo nell'ipotesi in cui ad emettere l'OEC sia un'autorità di emissione diversa rispetto a quelle individuate all'art. 4, par. 3, lett. a) della proposta di Regolamento.

La seconda fase, detta di esecuzione, è formata dalle attività volte a verificare da parte del destinatario la sussistenza delle condizioni per l'emissione dell'OEC e a conservare i dati richiesti al fine di impedire la rimozione, la cancellazione o la modifica dei dati per il tempo ritenuto congruo, e comunque non oltre i sessanta giorni, salvo l'avvio del procedimento finalizzato alla produzione dei dati congelati. La fase si apre con la ricezione dell'EPOC-PR da parte del privato e si può concludere con esiti alternativi: a) cessazione della conservazione dei dati dopo sessanta giorni; b) cessazione della conservazione a seguito della comunicazione dell'autorità di emissione ove si informa della carenza di necessità della conservazione; c) conservazione del dato, anche oltre i sessanta giorni, per il tempo necessario alla sua produzione, a seguito della notificazione della richiesta di produzione; d) dichiarazione da parte del privato dell'impossibilità materiale all'esecuzione e conseguente ritiro dell'OEC da parte dell'autorità di emissione. Protagonisti di questa fase sono l'autorità di emissione ed il privato, nella figura del rappresentante legale designato dal prestatore di servizi o, se non designato, del prestatore di servizi presso qualsiasi stabilimento.

L'ordine europeo di conservazione può essere emesso da un giudice, un organo giurisdizionale, un pubblico ministero o un altro magistrato inquirente competente nel caso interessato. Dunque, l'OEC può essere adottato da qualsiasi autorità giudiziaria: non solo dal giudice che procede, ma anche dall'ufficio del pubblico ministero¹¹¹⁷.

La scelta di legittimare anche l'ufficio del pubblico ministero all'emissione del provvedimento si giustifica perché l'OEC è un atto dal carattere servente, prodromico e funzionale alla successiva richiesta di produzione. L'OEC è stato pensato come uno strumento che consente alle autorità giudiziarie di agire con rapidità. Si è ritenuto di consentire all'ufficio del pubblico ministero di emettere, autorizzare o convalidare un OEC perché in ogni caso, per la successiva produzione del dato, sarà necessaria una nuova

procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione, cit., p. 79.

¹¹¹⁷ In tal senso, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1347; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 284.

richiesta, con conseguente nuovo esame delle condizioni di emissione del provvedimento¹¹¹⁸.

In effetti, il congelamento del dato non consente la *discovery* dell'informazione di cui è portatore il dato elettronico, né abilita il privato a produrre sempre e comunque il dato, non essendo uno strumento di trasferimento di esso. Dunque, avrebbe un impatto ridotto o comunque scarsamente afflittivo dei diritti fondamentali¹¹¹⁹. Da qui, la scelta di una disciplina più permissiva nei confronti dell'autorità.

Orbene, di recente ci si è chiesti, in un caso relativo all'ordine europeo di indagine, se rientra nelle nozioni di «autorità giudiziaria» e di «autorità di emissione» il pubblico ministero di uno Stato membro o, più in generale, la procura di uno Stato membro, indipendentemente dal rapporto di subordinazione legale che potrebbe esistere tra tale pubblico ministero o tale procura e il potere esecutivo dello Stato membro in questione, e dall'esposizione di detto pubblico ministero o di detta procura al rischio di essere soggetti, direttamente o indirettamente, ad ordini o istruzioni individuali da parte del suddetto potere¹¹²⁰. La Corte di giustizia si è pronunciata positivamente.

Le profonde similitudini relative alla formulazione dell'art. 1, par. 1, e dell'art. 2, lett. c), della direttiva 2014/41/UE con la formulazione dell'art. 4 della proposta di Regolamento relativo agli ordini europei di produzione e conservazione consentono di pervenire ad una conclusione del tutto analoga anche per l'autorità di emissione dell'OEC, mediante un'interpretazione testuale, contestuale e teleologica.

Dunque, anche per l'OEC si potrebbe ritenere che rientri nella nozione di «autorità di emissione» il pubblico ministero di uno Stato membro o, più in generale, la procura di uno Stato membro, indipendentemente dal rapporto di subordinazione legale che potrebbe esistere tra tale pubblico ministero o tale procura e il potere esecutivo di tale Stato membro, e dall'esposizione di detto pubblico ministero o di detta procura al rischio di essere soggetti, direttamente o indirettamente, ad ordini o istruzioni individuali da parte del predetto potere.

È considerata autorità di emissione anche qualsiasi altra autorità, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale. Tuttavia, in tal caso è previsto l'intervento di un'autorità di convalida che esaminerà la conformità del provvedimento alle condizioni di emissione¹¹²¹.

¹¹¹⁸ Sul punto, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 79.

¹¹¹⁹ Nel senso di uno strumento che ha un'incidenza inferiore sui diritti fondamentali rispetto all'OEP e, per questo, sono state previste condizioni meno stringenti per l'emissione, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 15.

¹¹²⁰ Cfr., Corte di giustizia, sentenza dell'8 dicembre 2020, causa C-584/19, *A. e A.* Per un commento, in dottrina, M. LANOTTE, *Il requisito dell'indipendenza del pubblico ministero nell'emissione di un ordine europeo di indagine*, in *Cass. pen.*, 3, 2021, p. 1060 ss.; S. QUATTROCOLO, *Nozioni autonome o variabili? La Corte di giustizia e la definizione di «autorità giudiziaria» e «autorità emittente» nel sistema della cooperazione giudiziaria infraeuropea. Riflessioni a margine di due recenti pronunce*, cit., p. 1792 ss. Sullo stesso tema, volendo, A. GAUDIERI, *Conformità del rapporto di subordinazione del pubblico ministero con la direttiva 2014/41/UE: l'orientamento adottato dalla Corte di giustizia nella sentenza A. e A.*, cit., p. 1 ss., disponibile al link: <https://www.unisa.it/uploads/14394/audieri.dic.2020.nota.pdf>.

¹¹²¹ Così, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 15; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1347.

L'autorità di convalida è un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero dello Stato di emissione. Dunque, possono essere autorità di convalida le stesse autorità di emissione individuate per gli OEC all'art. 4, par. 3, lett. a) della proposta di Regolamento, qualora ad emettere un OEC sia una autorità competente diversa che agisca in qualità di autorità inquirente. L'autorità di convalida può essere ritenuta autorità di emissione ai fini della trasmissione dell'OEC.

Se ne ricava che all'emissione di un OEC deve sempre partecipare un'autorità giudiziaria in veste o di autorità di emissione o di autorità di convalida.

Nella prima fase, l'autorità di emissione emette un OEC qualora siano soddisfatte tutte le condizioni indicate dall'art. 6 della proposta di Regolamento. In particolare, l'ordine deve essere necessario e proporzionato in relazione allo scopo del provvedimento, volto a neutralizzare il pericolo di rimozione, cancellazione o modifica dei dati elettronici. Non è prevista, quale condizione, la gravità del reato. Infatti, un OEC può essere emesso per qualsiasi tipo di reato e per l'esecuzione di una pena detentiva o di una misura di sicurezza privativa della libertà di almeno quattro mesi.

Vi è chi ha espresso delle perplessità relative all'assenza di una soglia di gravità del reato. Siccome l'OEC è un provvedimento tendenzialmente prodromico rispetto ad un successivo OEP, o un ordine europeo d'indagine o una richiesta di assistenza giudiziaria, vi sarebbe il rischio che tali successivi provvedimenti non siano adottabili. Pertanto, si è proposto di prevedere l'introduzione di una soglia minima di gravità del reato per cui è congelabile il dato a cui si riferisce, parificandolo all'OEP¹¹²².

Tuttavia, andrebbe anche considerato che – a differenza, in effetti, dell'OEP – per l'ordine europeo di indagine e per le rogatorie non è prevista, quale condizione, la gravità del reato. Invero, l'ordine europeo di indagine può essere emesso per qualsiasi reato senza limiti di soglia¹¹²³. L'inserimento della condizione della gravità del reato per l'OEC svilirebbe la funzione dello strumento, perché non sarebbe attivabile in tutti i casi in cui il dato può essere congelato in vista dell'emissione di un ordine europeo di indagine o di una richiesta di assistenza giudiziaria.

Infatti, l'OEC ha ragione di esistere perché cristallizza un dato che, a causa del decorso del tempo, può andare perduto o essere alterato, in vista di un successivo provvedimento rogatorio¹¹²⁴. Proprio l'ordine europeo di indagine e le richieste rogatorie risultano essere i provvedimenti più lenti e quindi più rischiosi per l'acquisizione dei dati elettronici, qualora questi non siano congelati nel più breve tempo possibile.

Più che sul criterio della gravità del reato, bisognerebbe concentrarsi su una condizione diversa. Per evitare che i dati siano sempre e comunque congelati, si potrebbe pensare di inserire quale condizione una valutazione sui sufficienti indizi di reato, che guarda ad elementi aventi attitudine probatoria dimostrativi, allo stato degli atti, della commissione di un reato. In tal modo, si garantirebbero in concreto sia il principio di necessità sia il principio di proporzionalità, perché proprio dalla valutazione dei sufficienti indizi di reato genererebbero – seppur in parte – le motivazioni che spingono a ritenere il ricorso all'OEC necessario e proporzionato.

¹¹²² Per tale proposta, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 14.

¹¹²³ Così, anche, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1347.

¹¹²⁴ Cfr., *considerando* n. 36, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

Bisognerebbe, invece, chiedersi come mai la gravità del reato sia prevista come condizione per l'OEP, laddove non esiste per gli altri strumenti di stampo rogatorio. Probabilmente il legislatore europeo, in applicazione del principio di proporzionalità, ha previsto un innalzamento delle garanzie per uno strumento che consente il rapporto diretto tra l'autorità pubblica ed il privato (e che, dunque, maggiormente espone i diritti fondamentali al pericolo di lesione), laddove si evitano altri meccanismi di garanzia come il riconoscimento del provvedimento da parte dell'autorità di esecuzione, come previsto per l'ordine europeo d'indagine.

Altro presupposto è previsto dal combinato disposto dall'art. 6, par. 1 e art. 5, par. 6-*bis* della proposta di Regolamento, secondo cui, in virtù della particolare sensibilità di essi, i dati conservati o trattati come parte di un'infrastruttura fornita da un prestatore di servizi a un'autorità pubblica possono essere oggetto di un OEC soltanto se l'autorità pubblica per la quale i dati sono conservati o trasformati si trova nello Stato di emissione.

Il provvedimento, oltre alla motivazione in punto di necessità e proporzionalità della misura, deve contenere: i dati relativi all'autorità di emissione e, laddove applicabile, all'autorità di convalida; il destinatario dell'ordine europeo di conservazione; le generalità dell'utente a cui si riferiscono i dati elettronici, eccetto i casi in cui l'unico fine dell'ordine è identificare l'utente, o qualsiasi altro identificativo univoco come il nome utente, l'ID o il nome dell'account per determinare i dati ricercati; la categoria dei dati da conservare; se del caso, l'intervallo di tempo per il quale è richiesta la conservazione; ed, infine, le disposizioni di diritto penale applicabili dello Stato di emissione.

Si tratta di informazioni obbligatorie utili per la corretta individuazione da parte dei prestatori di servizi dei dati di cui si chiede la conservazione¹¹²⁵. Tuttavia, nel certificato EPOC-PR da inviare al prestatore di servizi non vanno indicati i motivi della necessità e della proporzionalità della misura o altri dettagli sul caso per non compromettere le indagini¹¹²⁶.

Evidentemente, scopo della motivazione è quella di fungere da “cartina di tornasole” per un eventuale controllo endoprocessuale: la motivazione serve all'autorità di convalida, nel caso in cui sia necessario tale atto, per effettuare le operazioni di controllo richieste sull'attività richiesta dall'autorità di emissione; serve all'indagato o imputato per contestare successivamente l'ordine durante il procedimento penale, al fine di vedersi riconosciuti dei diritti e delle garanzie lese; serve al procedimento stesso per garantire la legalità in concreto ed assicurare la correttezza e i canoni del giusto processo.

Una volta adottato il provvedimento, potrebbe essere necessaria la convalida, qualora ad emettere il provvedimento sia un'autorità individuata ai sensi dell'art. 4, par. 3, lett. b) della proposta di Regolamento¹¹²⁷. Dunque, un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero nello Stato di emissione potrebbero essere chiamati a svolgere una funzione di controllo e di garanzia in relazione al provvedimento, prima della trasmissione del certificato EPOC-PR.

Bisognerebbe chiedersi a chi spetta in ipotesi di convalida la compilazione del certificato EPOC-PR. Ai sensi dell'art. 8, par. 1 della proposta di Regolamento, sembrerebbe che spetti all'autorità di convalida completare, firmare e certificare che le

¹¹²⁵ R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1348.

¹¹²⁶ Cfr., *considerando* n. 38, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹²⁷ In tal senso, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724.

informazioni contenute nel documento siano accurate e corrette. Per cui, la funzione svolta dall'autorità di convalida si estenderebbe sino al momento di produzione del successivo certificato da trasmettere. Da qui, dunque, la riduzione a sistema che consente di ritenere autorità di emissione anche un'autorità di convalida ai sensi dell'art. 4, par. 4 della proposta di Regolamento.

La funzione di garanzia e controllo assunta dall'autorità di convalida consentirebbe di estendere il suo *status* sino a ricomprendere anche le funzioni proprie dell'autorità di emissione in senso stretto, alla luce della particolare attività in concreto svolta per il buon fine del procedimento di conservazione del dato elettronico.

Orbene, la procedura sin qui descritta permette di considerare la convalida uno strumento che assicura il pieno rispetto dei diritti fondamentali e, pertanto, dovrebbe essere ottenuta prima dell'emissione dell'ordine.

Tuttavia, ai sensi dell'art. 4, par. 5, della proposta di Regolamento, limitatamente ai dati relativi agli abbonati o agli accessi, in casi di urgenza debitamente giustificati, è possibile emettere un ordine senza previa convalida, se questa non possa essere ottenuta in tempo utile, a condizione che l'autorità di emissione possa emettere un ordine equipollente senza convalida in un analogo caso nazionale.

La deroga, basata sul principio della massima cooperazione accelerata, è possibile solo in casi eccezionali. È prevista, dunque, una convalida *ex post* alla trasmissione dell'EPOC-PR, e comunque non oltre le quarantotto ore, soltanto in casi di emergenza e solo se non è possibile ottenere per tempo la preventiva convalida da parte dell'autorità giudiziaria. Se la c.d. *ex-post validation* non è disposta, l'autorità emittente revoca immediatamente l'ordine.

Si tratterebbe di ipotesi in cui non è possibile contattare l'autorità di convalida per ottenere la convalida e la minaccia è talmente imminente da richiedere un intervento immediato¹¹²⁸. Tuttavia, si creano dubbi di interpretazione siccome non sono indicati i casi di urgenza¹¹²⁹. Potrebbero essere situazioni di estremo pericolo e di minaccia per la vita o l'integrità fisica di una persona o per un'infrastruttura critica¹¹³⁰.

Una volta emesso l'ordine, è necessario compilare il certificato di ordine europeo di conservazione in tutte le sue parti, utilizzando il modello in formato standardizzato, escludendo i dati sensibili, la motivazione in punto di necessità e proporzionalità e tutte le informazioni che possono compromettere la segretezza ed il buon esito delle indagini¹¹³¹.

L'EPOC-PR, debitamente firmato e certificato¹¹³², è trasmesso dall'autorità di emissione o a suo nome secondo modalità sicure ed affidabili, come piattaforme, posta

¹¹²⁸ Cfr., *considerando* n. 36-bis, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹²⁹ Sul punto, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 70 ss.

¹¹³⁰ Si tratterebbe di ipotesi relative ad attacchi terroristici o attacchi *ransomware* che possono paralizzare infrastrutture strategiche con un sistema ospedaliero, ovvero quando si indaga sugli *account* di posta elettronica utilizzati dai sequestratori di persona per comunicare con i familiari delle vittime al fine di ottenere un riscatto. La soluzione prospettata prova a dare una lettura coordinata e sistematica di varie fonti perché riprenderebbe quanto già indicato all'art. 3, par. 2, lett. c. del Secondo protocollo alla Convenzione sulla criminalità informatica per la definizione di emergenza.

¹¹³¹ In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 80.

¹¹³² Il certificato è tradotto in una lingua ufficiale dell'Unione europea accettata dal destinatario o, se non sia stata specificata nessuna lingua, è tradotto in una delle lingue ufficiali dello Stato membro in cui il rappresentante legale risiede o è stabilito.

elettronica protetta o altri canali protetti¹¹³³, che consentano al destinatario la verifica dell'autenticità dell'atto, la conservazione delle tracce del flusso di comunicazione e la certificazione del flusso delle comunicazioni¹¹³⁴. Dunque, a circolare effettivamente è il certificato EPOC-PR¹¹³⁵.

Per la trasmissione, è concesso a ciascuno Stato membro di designare una o più autorità centrali responsabili della trasmissione amministrativa dei certificati, degli ordini, nonché della trasmissione dell'altra corrispondenza ufficiale relativa ai certificati o agli ordini¹¹³⁶.

Il certificato EPOC-PR è indirizzato direttamente al rappresentante legale designato dal prestatore di servizi o, in sua assenza, a qualsiasi stabilimento del prestatore di servizi¹¹³⁷, secondo quanto stabilito dall'art. 7 della proposta di Regolamento¹¹³⁸.

¹¹³³ Cfr., *considerando* n. 39, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. In dottrina, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 16.

¹¹³⁴ Alcuni prestatori di servizi hanno già creato piattaforme per la presentazione delle richieste da parte delle autorità di emissione. Il Regolamento non impedirebbe l'uso di queste piattaforme, che offrono numerosi vantaggi, tra cui una trasmissione sicura dei dati e la possibilità di un'autenticazione rapida dell'emittente. Tuttavia, le piattaforme dovranno evolversi nel senso di consentire la presentazione dei certificati standard, così come previsti da Regolamento, senza chiedere dati aggiuntivi sull'ordine.

Anche le piattaforme istituite dagli Stati membri o dagli organi dell'Unione possono fornire mezzi sicuri di trasmissione e agevolare l'autenticazione degli ordini e la raccolta di statistiche. Pertanto, l'Unione europea ha pensato di modificare le piattaforme eCodex e SIRIUS per includere una connessione sicura ai prestatori di servizi ai fini della trasmissione dei certificati e, se del caso, delle risposte dei prestatori di servizi. In ogni caso, è necessario che le piattaforme siano in linea con le norme in materia di protezione dei dati personali.

¹¹³⁵ In tal senso, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 285.

¹¹³⁶ Cfr., art. 4, par. 6, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹³⁷ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1349 ss. Secondo l'A., con le modalità di trasmissione indicate, si instaura un rapporto diretto dell'autorità richiedente con una nuova figura di riferimento, individuata nel rappresentante legale, senza l'intervento delle autorità del Paese in cui il prestatore di servizi è stabilito o rappresentato, «dandosi così vita ad una peculiare modulazione (fin qui inedita) del principio del mutuo riconoscimento giustificata in virtù di esigenze di speditezza, oltre che della considerazione che generalmente la conservazione dei dati non comporta alcun controllo da parte dello Stato nel cui territorio gli stessi sono detenuti, essendo nella maggior parte dei casi, inverso, il luogo di conservazione determinato dal prestatore di servizi sulla base di considerazioni meramente commerciali».

¹¹³⁸ Del "pacchetto" di proposte relative alla prova elettronica transnazionale fa parte anche la proposta di direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali. La proposta mira ad armonizzare i vari approcci nazionali che al momento comprendono: stabilire la giurisdizione nazionale su un prestatore di servizi sulla base della sua sede, del luogo in cui offre i servizi o dell'ubicazione dei suoi dati; estendere la competenza esecutiva (extraterritorialità); oppure richiedere che sia designato, per lo Stato membro in questione, un rappresentante speciale per alcuni prestatori di servizi. Secondo la proposta, il rappresentante legale dovrebbe risiedere o essere stabilito in uno degli Stati membri in cui il prestatore di servizi è stabilito o offre servizi, i suoi obblighi si limitano strettamente alla ricezione di decisioni e ordini emessi dalle autorità competenti degli Stati membri e all'ottemperanza agli stessi e può essere oggetto di procedure di esecuzione. Inoltre, gli Stati membri dovrebbero anche provvedere affinché un prestatore di servizi che offre servizi sul loro territorio ma che non è stabilito nell'Unione designi almeno un rappresentante legale nell'Unione ai fini della ricezione, dell'ottemperanza e dell'esecuzione di decisioni e ordini emessi dalle autorità competenti degli Stati membri per acquisire prove nei procedimenti penali. Il rappresentante legale risiede o è stabilito in uno degli Stati membri in cui il prestatore di servizi offre i servizi. Una simile direttiva dovrebbe avere un duplice effetto positivo: spingere i *service providers* a dotarsi di un apparato

Con la trasmissione dell'EPOC-PR al rappresentante legale o allo stabilimento del prestatore di servizi si chiude la fase di emissione e si apre la fase dell'esecuzione, descritta all'art. 10 della proposta di Regolamento. Quindi, l'atto con cui si realizza il passaggio di fase è la trasmissione. Tenuto conto dei mezzi di trasmissione, si dovrebbe ritenere che la recezione da parte del privato sia tendenzialmente contestuale e simultanea alla trasmissione stessa.

Nella fase di esecuzione il *dominus* è il destinatario dell'EPOC-PR, il quale, ricevuto il certificato, deve provvedere alla conservazione dei dati richiesti senza indebito ritardo¹¹³⁹. Prima di congelare i dati, dovrà effettuare una verifica sulla base delle informazioni ottenute mediante il certificato. La conservazione dei dati potrebbe essere rifiutata in tre casi.

In un primo caso, il certificato potrebbe non essere completo o contenere errori manifesti ovvero informazioni insufficienti per eseguirlo¹¹⁴⁰. Al verificarsi di tale circostanza, dovrebbe aprirsi una breve “finestra di dialogo” tra l'*internet service provider* e l'autorità di emissione.

Invero, il prestatore di servizi dovrebbe senza indebito ritardo chiedere chiarimenti, utilizzando il modulo di cui all'allegato III della proposta di Regolamento relativo alle informazioni sull'impossibilità di eseguire¹¹⁴¹, mentre l'autorità di emissione dovrebbe produrre i necessari chiarimenti entro cinque giorni per consentire al destinatario di ottemperare all'obbligo.

In secondo luogo, il destinatario potrebbe anche ritrovarsi nell'impossibilità materiale di ottemperare all'obbligo di conservazione a causa di circostanze non determinate dal destinatario stesso o dal prestatore di servizi. Si tratterebbe di ipotesi in cui i dati già siano stati cancellati o siano diventati per qualsiasi altro motivo inconservabili ovvero i dati richiesti non riguarderebbero informazioni elettroniche in possesso del prestatore di servizi o per suo conto al momento della ricezione dell'EPOC-PR¹¹⁴². In tali casi, il

organizzativo adeguato a soddisfare le frequenti richieste probatorie provenienti dagli Stati membri e consentire alle autorità nazionali di sapere con precisione come e a chi rivolgersi per ottenere il materiale probatorio di cui necessitano. Sull'argomento, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 290 ss.; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 63 ss. Cfr., Proposta di direttiva del Parlamento europeo e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali, Strasburgo, COM/2018/226 final - 2018/0107 (COD).

¹¹³⁹ Il legislatore europeo non ha inserito un preciso termine entro il quale va eseguito l'OEC, ma ha preferito una formula ampia e generica che può dare spazio ad azioni discrezionali. La dottrina, su tale scelta è particolarmente scettica tanto da ritenere che «mentre il legislatore UE è stato particolarmente preciso nell'individuazione del termine d'esecuzione dell'ordine di produzione, non si comprende tale generica scelta rivolta all'ordine di conservazione che pure condivide con l'ordine di produzione la stessa *ratio*». Cfr., E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2725.

¹¹⁴⁰ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 16.

¹¹⁴¹ Il modulo rappresenta «lo strumento formale attraverso cui deve svolgersi il dialogo tra il destinatario e l'autorità di emissione per qualsiasi questione inerente all'esecuzione dei certificati». Cfr., R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 80.

¹¹⁴² Si ritiene che l'impossibilità materiale sia presunta se la persona i cui dati sono ricercati non è cliente del prestatore di servizi o non può essere identificato come tale anche dopo una richiesta di ulteriori informazioni all'autorità di emissione, o se i dati sono stati legalmente cancellati prima della recezione

destinatario, senza indebito ritardo, informa l'autorità di emissione dell'impossibilità di eseguire l'ordine, spiegandone i motivi, utilizzando il modulo di cui all'allegato III della proposta di Regolamento relativo alle informazioni sull'impossibilità di eseguire.

Infine, l'art. 10, par. 6 della proposta di Regolamento inserisce una clausola di chiusura ampia e generica. Si prevede che in tutti i casi in cui, per altri motivi, non siano conservate le informazioni richieste, il destinatario, senza indebito ritardo, dovrà comunicarne i motivi all'autorità di emissione, utilizzando il modulo di cui all'allegato III della proposta di Regolamento relativo alle informazioni sull'impossibilità di eseguire.

La norma non chiarisce quali siano gli "altri motivi" che rendano ineseguibile un ordine, lasciando probabilmente un ampio margine di discrezionalità in capo al privato – circostanza che desta qualche perplessità – il quale sarà comunque tenuto a descrivere e motivare l'ineseguibilità nel modulo dedicato alle informazioni sull'impossibilità di eseguire da inviare all'autorità di emissione.

Dal modulo si evince che tra gli altri motivi è contemplato il rifiuto all'esecuzione qualora l'ordine di conservazione non sia stato emesso o convalidato da un'autorità di emissione conformemente all'art. 4 della proposta di Regolamento ovvero che il servizio non è coperto dalla proposta di Regolamento, come ad esempio i servizi giuridici, architettonici, ingegneristici e contabili forniti online a distanza.

Il modulo contiene anche una voce dedicata alla descrizione di qualsiasi altro motivo non elencato. Si potrebbe pensare ad ipotesi in cui l'ordine sia relativo a dati conservati o trattati come parte di un'infrastruttura fornita da un prestatore di servizi a un'autorità pubblica di cui è vietato il congelamento qualora l'autorità pubblica per la quale i dati sono conservati o trasformati non si trovi nello Stato di emissione.

Maggiore scetticismo dovrebbe manifestarsi per quanto riguarda la possibilità in capo al privato di non eseguire l'ordine perché la misura non è ritenuta necessaria o proporzionata, poiché si riconoscerebbe in capo al destinatario dell'ordine un potere eccessivo, proprio dell'autorità pubblica. In ogni caso, una simile concessione potrebbe comportare il rischio di paralizzare il sistema e dare adito a potenziali condotte dilatorie.

Ma cosa può fare l'autorità di emissione in caso di ineseguibilità? Di fondamentale importanza è il dialogo pubblico/privato e quindi il modulo relativo alle informazioni sull'impossibilità di eseguire, perché permette all'autorità di emissione di venire immediatamente a conoscenza delle circostanze che bloccano l'esecuzione e rivalutare la strategia investigativa¹¹⁴³.

Invero, l'autorità di emissione potrebbe ritirare l'ordine di conservazione qualora ritenga esaustive le motivazioni del destinatario. Altrimenti, ai sensi dell'art. 7, par. 4 della proposta di Regolamento, se ha indirizzato l'EPOC-PR ad un rappresentante legale e ritenga che questi non abbia ottemperato agli obblighi, può rivolgere l'OEC a qualsiasi stabilimento del prestatore di servizi nell'Unione, se sussiste un grave rischio di perdita dei dati¹¹⁴⁴.

Infine, l'autorità di emissione può attivare la procedura di modifica prevista all'art. 14 della proposta di Regolamento, con cui si instaura un procedimento simile a quello previsto per l'ordine europeo di indagine e di cui si parlerà *infra*.

dell'OEC. Cfr., *considerando* n. 41-bis, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹⁴³ In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 80.

¹¹⁴⁴ Cfr., *considerando* n. 37, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

La conservazione del dato dura ordinariamente sessanta giorni¹¹⁴⁵, trascorso il quale, non vi è più l'obbligo di congelamento¹¹⁴⁶. Nulla si dice sul giorno dal quale comincia a decorrere il termine. Tuttavia, siccome il destinatario è tenuto ad eseguire l'OEC senza indebito ritardo, si potrebbe individuare il *dies a quo* nella data di trasmissione e ricezione dell'EPOC-PR, ovvero, nei casi in cui vi siano elementi patologici che ne hanno inficiato l'esecuzione, dal momento in cui è possibile ottemperare all'obbligo.

I dati possono essere conservati anche per un termine inferiore o superiore¹¹⁴⁷. Invero, se la conservazione non è più necessaria, l'autorità di emissione informa il destinatario senza indebito ritardo, per evitare che i dati siano conservati inutilmente e a lungo; mentre, il prestatore di servizi è tenuto a conservare i dati oltre i sessanta giorni e fino alla produzione di essi, qualora l'autorità di emissione abbia confermato di aver avviato una richiesta di produzione mediante la procedura di assistenza giudiziaria, un OEP o un ordine europeo d'indagine¹¹⁴⁸. A tal fine, è necessario comunicare al destinatario anche l'avvio delle formalità finalizzate alla produzione e al trasferimento dei dati elettronici¹¹⁴⁹.

In conclusione, l'ordine europeo di conservazione è un provvedimento di garanzia, che evita la dispersione del dato elettronico o la sua alterazione. È uno strumento basato sul principio del mutuo riconoscimento, così come si sta evolvendo nello spazio di libertà sicurezza e giustizia. Il suo impiego è eventuale e strumentale alla successiva attivazione di una procedura *in rem* finalizzata all'apprensione ed al trasferimento del dato informatico avente attitudine probatoria nello Stato di emissione che lo ha richiesto e, pertanto, per essere efficace, deve essere una misura per quanto possibile segreta.

Dal conflitto tra libertà dei singoli ed esigenze di conservazione dei dati elettronici per futuri accertamenti nasce la volontà di proporzione, di ragionevolezza della misura e di equo bilanciamento tra gli interessi dei singoli e quelli della collettività su cui si basa l'intero impianto normativo relativo al pacchetto sulla formazione delle prove elettroniche nazionali nello spazio di libertà, sicurezza e giustizia.

Nell'applicare il principio di proporzionalità, e volendo graduare i sistemi di garanzia ed i limiti da porre agli strumenti che ontologicamente potrebbero ledere i diritti fondamentali in ragione dell'afflittività dello strumento, il legislatore europeo ha ritenuto, tra le varie articolazioni, che l'OEC sia il meccanismo meno afflittivo e, pertanto, ha

¹¹⁴⁵ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 16; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1352; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 81.

¹¹⁴⁶ Sull'argomento, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2727, secondo la quale il termine dei sessanta giorni, decorsi i quali il prestatore di servizi può cancellare i dati, se o è avviata una procedura volta alla produzione dei dati, è posto a protezione del diritto alla riservatezza dell'interessato.

¹¹⁴⁷ Così, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 81.

¹¹⁴⁸ In tal senso, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 16.

¹¹⁴⁹ Il periodo di sessanta giorni è ritenuto un termine congruo per consentire l'avvio di una richiesta ufficiale di produzione e trasferimento del dato elettronico. Per tale considerazione, cfr., *considerando* n. 42, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

previsto meccanismi compensativi meno solidi rispetto a quelli individuati per le varie forme di ordine di produzione.

7. L'ordine europeo di produzione

L'ordine europeo di produzione (OEP) è un provvedimento con cui, ai sensi dell'art. 2, n. 1) della proposta di Regolamento, un'autorità di emissione di uno Stato membro ingiunge di produrre prove elettroniche a un prestatore di servizi che offre servizi nell'Unione ed è stabilito o rappresentato in un altro Stato membro.

Si tratta di una decisione vincolante volta ad obbligare il destinatario a trasferire all'autorità richiedente dati elettronici utili ai fini dell'individuazione di persone o entità coinvolte in attività criminali o rilevanti per i procedimenti penali perché utilizzabili come prove.

Come per l'OEC, anche l'OEP prevede un contatto diretto tra l'autorità di emissione e un prestatore di servizi stabilito o rappresentato in un altro Stato membro, senza l'intervento di un'autorità di esecuzione, la quale interviene solo in casi eccezionali e residuali.

Tale meccanismo, basato su una visione evoluta del mutuo riconoscimento, o se si preferisce, su un *tertium genus* non inquadrabile sotto l'egida né del principio della mutua assistenza, né del mutuo riconoscimento, nel prevedere un rapporto diretto con i prestatori di servizi, senza ulteriori passaggi, assicura una procedura il più possibile snella ed efficiente, ottimizzando al massimo i tempi di ricerca e trasferimento prima che essa venga cancellata, distrutta o alterata¹¹⁵⁰.

Lo strumento ha un maggior impatto sui diritti fondamentali rispetto all'OEC e pertanto, in tutte le sue modulazioni, prevede maggiori garanzie. Il legislatore europeo sta quindi provando a creare uno strumento che sia attento alla tutela dei diritti fondamentali, operando un bilanciamento tra interessi contrapposti, alla luce del principio di proporzionalità.

La disciplina dell'ordine europeo di produzione è parzialmente diversa rispetto a quella prevista per l'OEC, perché si opera un distinguo in base alla tipologia dei dati oggetto dell'ordine, a causa del diverso impatto che questi hanno sui diritti fondamentali¹¹⁵¹.

Il procedimento si divide in due fasi: fase di emissione e fase di esecuzione.

La fase di emissione è dedicata all'emissione del provvedimento, alla compilazione ed alla trasmissione del certificato di ordine europeo di produzione (EPOC). Ha inizio con la valutazione delle condizioni per l'emissione dell'OEP e si conclude con la trasmissione dell'EPOC al privato o con un eventuale provvedimento di non convalida dell'OEP.

¹¹⁵⁰ E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724. V., inoltre, O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss., secondo i quali «l'istituzione di nuovi strumenti standard per l'acquisizione di prove, quali l'ordine europeo di produzione e l'ordine europeo di conservazione, intende evitare il dispendio di tempo e risorse necessari ad attuare forme di cooperazione che inevitabilmente seguono iter diversi per ciascuno dei paesi interessati».

¹¹⁵¹ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1342 ss.

Protagonisti della fase sono l'autorità di emissione e l'autorità di convalida, che interviene solo nelle ipotesi previste dal legislatore in cui è necessaria la convalida dell'OEP, ai sensi dell'art. 4, par. 1, lett. b) e par. 2, lett. b) della proposta di Regolamento. Ulteriore protagonista, il cui intervento è previsto solo in specifici e tassativi casi, è l'autorità competente nello Stato di esecuzione.

Con la fase di esecuzione si procede alla verifica delle condizioni per l'emissione dell'OEP da parte del destinatario ed al trasferimento dei dati elettronici all'autorità di emissione dello Stato richiedente. La fase si apre con la ricezione dell'EPOC da parte del destinatario ed, eventualmente, dell'autorità competente nello Stato di esecuzione e si può concludere con esiti alternativi: a) produzione dei dati elettronici entro dieci giorni o, in caso di emergenza, entro sei ore dalla ricezione del certificato; b) dichiarazione da parte del privato dell'impossibilità materiale all'esecuzione e conseguente ritiro dell'OEP da parte dell'autorità di emissione; c) ritiro dell'OEP da parte dell'autorità di emissione.

Nella seconda fase è previsto l'intervento dell'autorità di emissione, del destinatario dell'EPOC, nella figura del rappresentante legale designato dal prestatore di servizi o, se non designato, del prestatore di servizi presso qualsiasi stabilimento, e nelle ipotesi tassativamente individuate, dell'autorità di esecuzione, che interviene in qualità di soggetto eventuale del procedimento.

La maggiore invasività dello strumento¹¹⁵² – accentuata dalla circostanza per cui non è previsto un intervento obbligatorio dell'autorità di esecuzione che provveda al riconoscimento ed alla verifica del rispetto dei diritti fondamentali – ha comportato l'introduzione di un sistema di garanzie parzialmente diverso rispetto a quanto previsto per l'ordine europeo di indagine e sicuramente più incisivo rispetto all'OEC. La ricerca e produzione dei dati elettronici implica ontologicamente un impatto maggiore sui diritti fondamentali rispetto ad altre attività a carattere investigativo ed epistemologico-probatorio.

Innanzitutto, è d'uopo chiarire che all'autorità giudiziaria non è consentito imporre la produzione di dati che saranno registrati in futuro, né delegare intercettazioni in tempo reale di flussi informatici o telematici¹¹⁵³.

Non tutti i dati sono uguali. I dati elettronici riconducibili ad una persona, letti sistematicamente e globalmente, consentono di pervenire a conoscenze e ad informazioni che devono restare quanto più possibili riservate relative sia alla persona coinvolta nel procedimento penale sia a terzi. L'apporto conoscitivo del dato varia in base alla tipologia a cui esso afferisce.

Si può, dunque, parlare di eterogeneità e di diverso “spessore” delle varie informazioni digitali disponibili: al minor impatto conoscitivo dei dati relativi agli abbonati ed agli accessi, si contrappone la maggior incisività dei dati relativi alle operazioni ed al contenuto, solitamente rilevanti come materiale probatorio¹¹⁵⁴.

¹¹⁵² In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1343.

¹¹⁵³ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 9; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 72.

¹¹⁵⁴ Così, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 17; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1343; F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., 1 ss.; R.

Innanzitutto a questo fenomeno, in applicazione del principio di gradualità, il legislatore europeo ha ritenuto opportuno prevedere modulazioni diverse dello stesso strumento relativo alla produzione dei dati elettronici, in base alla tipologia di informazione ricavabile dal dato e, di conseguenza, dal diverso impatto sui diritti fondamentali.

Invero, i dati elettronici sono divisibili in due gruppi: i dati non relativi al contenuto e dati relativi al contenuto. Il legislatore europeo ha deciso di individuare quattro categorie di dati¹¹⁵⁵. I dati relativi agli abbonati¹¹⁵⁶, agli accessi¹¹⁵⁷ ed alle operazioni¹¹⁵⁸ farebbero

PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 71 ss.

¹¹⁵⁵ La distinzione ricalca per grandi linee quanto già previsto nella legislazione degli Stati Uniti d'America, negli ordinamenti giuridici di molti Stati membri e di Paesi terzi. Solo in parte corrisponderebbe a quanto previsto nella Convenzione sulla criminalità informatica.

¹¹⁵⁶ Secondo quanto previsto dall'art. 2, n. 7 della proposta di Regolamento, i dati relativi agli abbonati riguardano l'identità di un abbonato o di un cliente, come il nome, la data di nascita, l'indirizzo postale o geografico, i dati di fatturazione e pagamento, il numero di telefono o l'indirizzo e-mail forniti ovvero il tipo di servizio e la sua durata, compresi i dati tecnici e i dati che identificano le misure tecniche correlate o le interfacce usate dall'abbonato o dal cliente o a questo fornite e i dati connessi alla convalida dell'uso del servizio. Sono escluse le *password* o altri mezzi di autenticazione usati al posto di una *password*, forniti dall'utente o creati a sua richiesta.

¹¹⁵⁷ Ai sensi dell'art. 2, n. 8 della proposta di Regolamento, i dati relativi agli accessi riguardano l'inizio e la fine di una sessione di accesso dell'utente a un servizio strettamente necessari al solo fine di identificare l'utente del servizio, come la data e l'ora d'uso, o la connessione al servizio (log-in) e la disconnessione (log-off) dal medesimo, unitamente all'indirizzo IP assegnato all'utente dal prestatore di servizi di accesso a internet, ai dati che identificano le interfacce usate e all'identificativo utente. Di tale categoria fanno anche parte i metadati delle comunicazioni elettroniche quali i dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche compresi i dati usati per tracciare e identificare la fonte e il destinatario di una comunicazione, i dati relativi alla localizzazione del dispositivo generati nel contesto della fornitura di servizi di comunicazione elettronica nonché la data, l'ora, la durata e il tipo di comunicazione. Si tratterebbe di una categoria di dati intermedia tra i dati relativi agli abbonati e i dati relativi alle operazioni.

I metadati sono già stati sottoposti all'attenzione della Corte di giustizia, la quale ne ha confermato la sensibilità. Con la sentenza *Digital Rights Ireland*, la Corte di giustizia ha annullato la direttiva 2006/24/CE sulla conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. In particolare, la Corte di giustizia ha avuto modo di precisare che la direttiva 2006/24/CE non aveva violato il contenuto essenziale degli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, relativi al diritto alla vita privata e familiare e al diritto alla protezione dei dati personali. Tuttavia, la direttiva aveva arrecato una restrizione sproporzionata ai diritti fondamentali in esame. Invero, una simile raccolta di dati introduceva un sistema di sorveglianza di massa senza limiti di oggetto e senza l'indicazione di necessarie garanzie. Inoltre, la conservazione dei dati deve essere strettamente necessaria per combattere le forme gravi di criminalità e deve essere eseguita assicurando standard minimi di garanzia per assicurare una effettiva protezione contro i rischi di abusi o di accesso illegale alle informazioni. Il nucleo essenziale dei diritti fondamentali, però non era stato intaccato perché ad oggetto vi erano i metadati, geneticamente inadatti a rivelare il flusso di telecomunicazioni, pur permettendo, se conservati per un periodo di tempo apprezzabile, la ricostruzione di un profilo dettagliato dell'utente. Cfr., Corte di giustizia, sentenza 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*; in dottrina, G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, cit., p. 1607 ss.; S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Democrazia e Sicurezza*, 3, 2014, p. 1 ss.; C.M. CASCIONE, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della Corte di giustizia e gli echi del datagate*, in *Nuova giur. civ. comm.*, 11, 2014, p. 1044 ss.; R. FLOR, *La Corte di giustizia considera la direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, cit., p. 178 ss.; M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Dir. Un. Eur.*, 4, 2014, p. 803 ss.

¹¹⁵⁸ I dati relativi alle operazioni riguardano la fornitura di un servizio offerto da un prestatore di servizi e servono per fornire informazioni di contesto o supplementari sul servizio e che sono generati o trattati da

parte del gruppo dei dati non relativi al contenuto, mentre sono dati relativi al contenuto tutti i dati conservati in formato digitale, individuati in modo residuale, diversi dai dati relativi agli abbonati, agli accessi ed alle operazioni¹¹⁵⁹.

Sebbene tutte le categorie contengano dati personali e rientrino nel campo di applicazione delle garanzie sulla protezione dei dati¹¹⁶⁰, i dati relativi agli abbonati ed agli accessi hanno un impatto sui diritti fondamentali inferiore rispetto ai dati sulle operazioni e sul contenuto¹¹⁶¹. Pertanto, è stato previsto un regime “a doppio binario”¹¹⁶² con un grado di tutela più elevato per i dati relativi alle operazioni ed al contenuto¹¹⁶³.

I dati si distinguono anche per lo scopo per cui possono essere richiesti. Mentre i dati relativi agli abbonati ed agli accessi sono utili per ottenere i primi indizi in un'indagine sull'identità dell'indagato¹¹⁶⁴, i dati relativi alle operazioni e i dati relativi al contenuto sono i più pertinenti come materiale probatorio¹¹⁶⁵.

Inoltre, i dati relativi agli accessi rientrano nell'ambito di un'attività investigativa dove è di fondamentale importanza conoscere ed attuare azioni strategiche, perché se l'utente è ignoto, spesso occorre ottenere tali dati prima di poter richiedere al prestatore

un sistema di informazione del prestatore di servizi, come la fonte e il destinatario di un messaggio o altro tipo di interazione, i dati sull'ubicazione del dispositivo, la data, l'ora, la durata, le dimensioni, il percorso, il formato, il protocollo usato e il tipo di compressione, a meno che tali dati costituiscano dati relativi agli accessi. Di tale categoria fanno anche parte i metadati delle comunicazioni elettroniche quali i dati trattati in una rete di comunicazione elettronica per trasmettere, distribuire o scambiare il contenuto delle comunicazioni elettroniche compresi i dati usati per tracciare e identificare la fonte e il destinatario di una comunicazione, i dati relativi alla localizzazione del dispositivo generati nel contesto della fornitura di servizi di comunicazione elettronica nonché la data, l'ora, la durata e il tipo di comunicazione.

¹¹⁵⁹ Sarebbero i dati digitali relativi a testo, voce, video, immagine o suono, così come individuati – per esempi ed esclusioni – dall'art. 2, n. 10 della proposta di Regolamento. Cfr., O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss., secondo i quali il ricorso alla tecnica definitoria per esempi, che non chiarisce se l'elenco di esempi proposti sia esaustivo, solleverebbe serie riserve sul piano interpretativo.

¹¹⁶⁰ In tal senso, *Relazione alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, p. 15. In dottrina, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 72.

¹¹⁶¹ In tal senso, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 8; O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss.

¹¹⁶² Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1343, secondo la quale «Ne deriva un assetto parzialmente diversificato [...] della disciplina relativa all'emissione, alle condizioni di applicabilità, ai mezzi di ricorso, alle informazioni relative, nonché all'esecuzione degli ordini in questione. Resta fermo, tuttavia, sullo sfondo un comune *fil rouge*, inerente l'ambito di applicazione, che lega le diverse articolazioni dello strumento *de quo*, accomunandole sotto taluni profili fondamentali».

¹¹⁶³ In breve, qualora siano richiesti dati relativi alle operazioni ed al contenuto, è prevista la convalida qualora l'autorità di emissione sia l'ufficio del pubblico ministero e non è possibile attivare la procedura d'urgenza prevista all'art. 4, par. 5 della proposta di Regolamento. Ulteriori garanzie sono previste nel caso in cui tali dati siano protetti con immunità o privilegi o siano soggetti a norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione o che la loro divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza o la difesa nazionali.

¹¹⁶⁴ Appare evidente che i dati relativi agli accessi siano richiesti allo stesso scopo dei dati relativi agli abbonati ed abbiano un impatto simile sui diritti fondamentali. Pertanto, essi sono soggetti alle stesse condizioni dei dati relativi agli abbonati.

¹¹⁶⁵ Cfr., *considerando* n. 23, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*.

di servizi i dati relativi agli abbonati correlati a quell'identificatore¹¹⁶⁶. Tuttavia, a differenza dei dati sulle operazioni, da essi non è possibile ottenere informazioni sui contatti dell'utente e sul luogo in cui questo si trova, né possono servire per profilare il soggetto a cui si riferiscono i dati¹¹⁶⁷.

Tale distinzione si evince sia nella fase di emissione sia nella fase di esecuzione.

Per quanto attiene all'organo legittimato all'emissione, bisogna dividere le ipotesi in cui l'OEP abbia ad oggetto i dati relativi agli abbonati o agli accessi dall'ipotesi in cui l'OEP sia emesso per ottenere i dati relativi alle operazioni o al contenuto.

Ai sensi dell'art. 4, par. 1, della proposta di Regolamento, nel caso di dati relativi agli abbonati o agli accessi, l'autorità di emissione di un OEP può essere un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato¹¹⁶⁸. Tuttavia, può emettere un OEP anche qualsiasi altra autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale, purché la decisione sia convalidata a seguito di un esame della conformità delle condizioni di emissione di un OEP da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero nello Stato di emissione¹¹⁶⁹.

¹¹⁶⁶ Cfr., *considerando* n. 21, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹⁶⁷ Cfr., *considerando* n. 22, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale. Critici sulla distinzione in dati relativi agli accessi e dati relativi alle operazioni, O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss., secondo cui «la mancata menzione di determinate tipologie di dati non permette una loro agevole collocazione, stante anche l'elevata probabilità di sovrapposizioni, quantomeno tra la categoria dei dati relativi agli accessi e i dati relativi alle operazioni». Invero, l'ambiguità sull'appartenenza di determinate informazioni all'una o all'altra categoria di dati può provocare un'incertezza giuridica. Pertanto, sarebbe auspicabile o provvedere ad una puntuale e lineare definizione delle categorie di dati o alla rimozione delle differenze di regime.

¹¹⁶⁸ Critico sul punto, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1287, secondo cui la proposta appare eccezionale perché non assicurerebbe una piena attuazione del controllo giurisdizionale, permettendo al pubblico ministero di emettere un OEP avente ad oggetto dati relativi ad abbonati e agli accessi. Infatti, un vaglio giurisdizionale preventivo è assicurato per i soli ordini di produzione di dati relativi alle operazioni ed al contenuto, mentre per gli ordini di produzione dei dati relativi agli abbonati ed agli accessi è possibile solo un ricorso *ex post* davanti ad un organo giurisdizionale dello Stato di emissione in conformità alla *lex fori*. Del resto, recentemente, anche la giurisprudenza della Corte europea dei diritti dell'uomo ha ritenuto necessario prevedere dei meccanismi di garanzia e controllo da parte di un organo giurisdizionale indipendente delle operazioni istruttorie invasive della *privacy*. Cfr., Corte EDU, 27 settembre 2018, *Brazzi c. Italia*, ricorso n. 55278/11, punto 1 ss. Per un commento alla sentenza, R. CHENAL, *Il diritto al rispetto del domicilio in caso di perquisizione (art. 8 CEDU)*, in AA.VV., *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno (2016-2020)* (a cura di A. DI STASI), Milano, 2020, p. 645 ss.; D. CARDAMONE, *La sentenza della Cedu Brazzi c. Italia: sono arbitrarie le perquisizioni disposte dall'Autorità giudiziaria?*, in *Questione Giustizia*, 15 gennaio 2019, p. 1 ss. In giurisprudenza, v., inoltre, Corte EDU, 16 maggio 2019, *Halabi c. Francia*, ricorso n. 66554/14; Corte EDU, 2 ottobre 2014, *Delta Pekárny a.s. c. Russia*, ricorso n. 97/11; Corte EDU, 15 ottobre 2013, *Gutsanovi c. Bulgaria*, ricorso n. 34529/10; Corte EDU, 21 febbraio 2008, *Ravon e altri c. Francia*, ricorso n. 18497/03; Corte EDU, 30 settembre 2008, *Işildak c. Turchia*, ricorso n. 12863/02.

¹¹⁶⁹ In sostanza, la regola coincide con quella prevista per gli ordini europei di conservazione. Cfr., in dottrina, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-*

Diversamente, secondo quanto stabilito dall'art. 4, par. 2, della proposta di Regolamento, un OEP avente ad oggetto dati relativi alle operazioni o al contenuto – dunque, ontologicamente più sensibili – può essere emesso senza necessaria convalida soltanto da un'autorità giurisdizionale¹¹⁷⁰, restandone escluso l'ufficio del pubblico ministero. Qualora sia emesso da un'autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale (come, ad esempio, può essere un pubblico ministero), l'OEP dovrà essere convalidato da un giudice, un organo giurisdizionale o un magistrato inquirente¹¹⁷¹.

La distinzione confermerebbe la maggior attenzione verso la produzione di dati dal carattere più sensibile e più intrusivi della sfera della dignità della persona mediante l'individuazione della competenza in capo a organi depositari di maggiori garanzie. Il doppio binario “garantistico” sarebbe confermato anche dalla disciplina relativa alla *ex post validation*.

Invero, solamente per gli OEP aventi ad oggetto dati relativi ad abbonati o agli accessi, qualora gli ordini siano emessi da un'autorità competente che agisca in qualità di autorità inquirente nel procedimento penale ai sensi dell'art. 4, par. 1, lett. b) della proposta di Regolamento, e dunque, non si tratti di un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero, è possibile, in caso di urgenza, richiedere la convalida *ex post* senza indebito ritardo, o comunque entro quarantotto ore dall'emissione, a condizione che si ritenga che la convalida non possa essere ottenuta in tempo utile e che l'autorità di emissione sia legittimata ad emettere ordini senza convalida in casi interni analoghi¹¹⁷².

Dunque, presupposti per la procedura di emissione con convalida *ex post* sono: l'emissione di un OEP avente ad oggetto i dati relativi agli abbonati o agli accessi; i casi di urgenza; l'impossibilità di ottenere una convalida in tempo utile; la possibilità di emettere un ordine senza convalida in casi analoghi nazionali¹¹⁷³.

Qualora la convalida successiva non sia concessa, l'autorità di emissione revoca immediatamente l'ordine e, conformemente al suo diritto nazionale, provvede a cancellare gli eventuali dati acquisiti o garantisce che non siano usati come prove. Se ne

evidence, cit., p. 1347; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 70; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 8.

¹¹⁷⁰ In particolare, un giudice, un organo giurisdizionale o un magistrato inquirente competente nel caso interessato. Sul punto, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 284; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 70.

¹¹⁷¹ Come per l'OEC, anche per l'OEP l'autorità di convalida può essere considerata autorità di emissione ai fini della trasmissione del relativo certificato, ai sensi dell'art. 4, par. 4 della proposta di Regolamento.

¹¹⁷² In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 70.

¹¹⁷³ Il legislatore europeo anche in tal caso non ha indicato cosa si intenda per urgenza e quali siano i casi in cui è impossibile ottenere una convalida in tempo utile. Si dovrebbe ritenere che si tratti di ipotesi in cui la minaccia sia talmente imminente da richiedere un intervento immediato. Potrebbero essere situazioni di estremo pericolo e di minaccia per la vita o l'integrità fisica di una persona o per un'infrastruttura critica, così come indicato per i casi di emergenza previsti dal Secondo Protocollo sulla criminalità informatica.

ricava che, se i dati ottenuti senza convalida – per qualsiasi ragione – dovessero far ingresso nel procedimento penale, dovrebbero essere dichiarati inutilizzabili.

Un OEP può essere emesso se sono soddisfatte tutte le condizioni indicate all'art. 5 della proposta di Regolamento¹¹⁷⁴. È possibile suddividere le condizioni in generali e specifiche e in condizioni *ex ante* e condizioni *ex post*. Le condizioni generali valgono per qualsiasi OEP, mentre le condizioni specifiche sono individuate in base alla tipologia di dato informatico da richiedere.

Dal punto di vista logico, ma non strettamente temporale perché la valutazione dovrebbe apparire contestuale, l'autorità di emissione dovrebbe verificare la sussistenza prima di tutte le condizioni generali e, solo dopo aver concluso positivamente, dovrà verificare la presenza in concreto anche delle condizioni specifiche.

Innanzitutto, l'OEP deve essere necessario e proporzionato ai fini del procedimento penale per cui si richiedono o per l'esecuzione di misure di sicurezza privative della libertà o di pene detentive che non sono state rese in contumacia in caso di latitanza del condannato.

Si richiederebbe, dunque, una valutazione in concreto della necessità e della proporzionalità delle misure adottate con il provvedimento. In altre parole, l'autorità di emissione deve considerare se l'ordine è limitato a quanto necessario per raggiungere il legittimo obiettivo di ottenere i dati pertinenti e necessari che dovranno servire solo nella singola fattispecie, tenendo debitamente conto dell'impatto del provvedimento sui diritti fondamentali della persona i cui dati sono richiesti¹¹⁷⁵.

In pratica, l'autorità di emissione, in via preliminare, deve effettuare «un'equilibrata ponderazione tra gli obiettivi che si propone di raggiungere con l'emissione dell'ordine ed il sacrificio che l'adozione di questo comporta per i diritti individuali dei soggetti coinvolti»¹¹⁷⁶.

Sebbene i requisiti possano apparire piuttosto generici¹¹⁷⁷, vi è chi ritiene che praticamente debbano essere identificati con le condizioni di emissione degli atti istruttori corrispondenti che opererebbero a livello nazionale, in base alle regole della *lex fori*¹¹⁷⁸.

Ulteriore condizione è la previsione di una misura dello stesso tipo per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione¹¹⁷⁹.

A queste due condizioni generali *ex ante* si affianca una condizione specifica, indicata per la tipologia di dato da richiedere, in applicazione del principio di gradualità, che – come già chiarito – appare un corollario del principio di proporzionalità.

¹¹⁷⁴ Sull'argomento, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 285; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 76.

¹¹⁷⁵ Cfr., considerando n. 29, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹⁷⁶ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1345.

¹¹⁷⁷ Così, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 293.

¹¹⁷⁸ Sul punto, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1285.

¹¹⁷⁹ In Italia, in linea di massima, il riferimento sarebbe in generale alla disciplina relativa ai sequestri ed in particolare ai sequestri di dati informatici presso i fornitori di servizi informatici, telematici e di telecomunicazioni prevista all'art. 254-bis c.p.p. e all'acquisizione dei dati telematici prevista all'art. 132, d.lgs. 30 giugno 2003, n. 196. Sull'argomento, M. PITTIRUTI, *Digital evidence e procedimento penale*, cit., p. 43 ss.

In particolare, nell'ipotesi di dati relativi agli abbonati o agli accessi, l'OEP può essere emesso per qualsiasi reato¹¹⁸⁰ e per l'esecuzione di una pena detentiva o una misura di sicurezza privativa della libertà di almeno quattro mesi. Sistemáticamente, la condizione va valutata alla luce anche della condizione generale secondo la quale l'OEP può essere emesso solo in caso di misura dello stesso tipo disponibile per lo stesso reato in un caso interno analogo. Infatti, nonostante l'OEP avente ad oggetto i dati relativi agli abbonati o agli accessi possa essere emesso per tutti i reati, per tali reati deve comunque essere possibile attivare una misura analoga in una situazione nazionale comparabile.

Diversa, invece, la scelta operata nell'ipotesi in cui un OEP abbia ad oggetto dati relativi alle operazioni o al contenuto. Sono individuati requisiti più rigorosi onde tener conto della natura più sensibile di tali dati e del corrispondente maggiore impatto dell'ordine rispetto ai dati relativi agli abbonati o agli accessi¹¹⁸¹.

In tali casi, il legislatore ha preferito che i dati siano ottenibili mediante OEP solo per i reati più gravi individuati secondo un criterio quantitativo e qualitativo¹¹⁸².

Ed invero, secondo il criterio quantitativo, è possibile emettere un OEP per la produzione di dati relativi alle operazioni o al contenuto solo per reati punibili nello Stato di emissione con una pena detentiva superiore nel massimo a tre anni¹¹⁸³.

La soglia basata sulla durata massima della pena detentiva consente un approccio proporzionato, insieme a una serie di altre condizioni e garanzie *ex ante* ed *ex post* per assicurare il rispetto della proporzionalità e dei diritti degli interessati. Inoltre, l'ambito di applicazione dello strumento sarebbe circoscritto ai reati più gravi senza limitare eccessivamente la possibilità di uso dello strumento da parte degli operatori del settore. Infine, si escluderebbero dall'ambito di applicazione un'ampia serie di reati che dipende da ogni singolo codice penale nazionale¹¹⁸⁴.

In dottrina si è anche affermato che il limite edittale sia piuttosto basso e consente di ricomprendere la maggioranza delle fattispecie penali, annullando di fatto la differenza tra gli OEP aventi ad oggetto dati relativi ad abbonati o agli accessi e gli OEP aventi ad oggetto dati relativi alle operazioni o al contenuto. Tuttavia, non apparirebbe un difetto grave se si considera che, generalmente, nell'ordinamento interno le indagini informatiche possono essere eseguite per qualsiasi tipo di reato¹¹⁸⁵.

¹¹⁸⁰ Così, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 285.

¹¹⁸¹ In tal senso, *Relazione alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, p. 17.

¹¹⁸² Su tale distinzione, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1347.

¹¹⁸³ Così, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 18; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1347 ss.; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 284 ss.; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 76.

¹¹⁸⁴ Cfr., *Relazione alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, p. 17. In altre parole, sarebbero esclusi dall'ambito di applicazione un numero significativo di reati che gli Stati membri considerano meno gravi e puniscono con una pena massima inferiore. Il criterio quantitativo avrebbe, infine, il vantaggio di essere facilmente applicabile nella pratica.

¹¹⁸⁵ Sul punto, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1286, il quale, tra l'altro, ritiene

Il requisito, inoltre, è in linea con la disciplina interna relativa alla *data retention*, secondo cui i dati possono essere acquisiti per procedimenti relativi a reati sanzionati con la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni¹¹⁸⁶, e per altri reati individuati mediante un criterio qualitativo.

Sono individuati, secondo il criterio qualitativo, una serie di reati particolarmente riprovevoli per cui è possibile richiedere la produzione di dati relativi alle operazioni ed al contenuto, se commessi in tutto o in parte a mezzo di un sistema di informazione¹¹⁸⁷, a prescindere dalla pena edittale prevista.

Bisognerebbe riflettere se da una lettura sistematica di tali condizioni siano soddisfatti non solo il principio di necessità e proporzionalità¹¹⁸⁸, ma anche il principio di uguaglianza, e ciò in ragione di codici nazionali – penali e di procedura penale – non perfettamente armonizzati.

Le scelte compiute dal legislatore europeo manifesterebbero la tensione tra il principio di uguaglianza ed il principio di sovranità statale. In pratica, per evitare che la misura diventi strumenti di disuguaglianza se comparata tra casi interni analoghi e casi caratterizzati da elementi transfrontalieri, rischia però di generare disuguaglianze se la misura è valutata comparando i casi caratterizzati da elementi transfrontalieri così come perseguiti in Stati diversi, ove la gravità del reato potrebbe essere valutata diversamente.

Dunque, una riflessione andrebbe fatta sulla razionalità delle condizioni – in particolare, quelle specifiche – valutando se siano in linea con le misure strettamente interne e se vi sia un apprezzabile rischio di disparità di trattamento. Sulla scorta di tali considerazioni, sarebbe opportuno creare un sistema di cooperazione giudiziaria effettivamente armonico.

Una ulteriore restrizione è prevista nel caso di dati trattati per un'autorità pubblica¹¹⁸⁹, in ragione della particolare sensibilità dei dati. In tal caso, un ordine europeo di produzione relativo a dati conservati o trattati come parte di un'infrastruttura fornita da

comprensibile «la scelta di rinunciare al tradizionale requisito della doppia incriminazione. Ad esso deroga già la disciplina sull'ordine europeo di indagine penale, la quale consente la raccolta delle prove all'estero in rapporto a tutti i reati appositamente elencati in una lista (art. 11 § 1 lett. g della direttiva 2014/41 e 11 d.lgs. n. 108/2017)».

¹¹⁸⁶ Cfr., art. 132, comma 3, d.lgs. 30 giugno 2003, n. 196.

¹¹⁸⁷ Tra le altre cose, la proposta di Regolamento fa riferimento ai reati previsti nella decisione quadro 2001/413/GAI, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. Tuttavia, la decisione quadro è stata sostituita dalla direttiva 2019/713/UE del 17 aprile 2019, che ha aggiornato ed integrato il catalogo di reati, prevedendo nuove disposizioni in materia di reati, con riferimento in particolare alla frode informatica. Si fa poi riferimento ai reati relativi all'abuso ed allo sfruttamento sessuale dei minori nonché alla pornografia minorile, ai reati nel settore degli attacchi contro i sistemi informatici e, infine, ai reati di terrorismo, ai reati riconducibili a un gruppo terroristico ed ai reati connessi alle attività terroristiche.

¹¹⁸⁸ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 18 ss. Secondo l'A., la scelta del legislatore di individuare un criterio quantitativo ed un criterio qualitativo sembra essere giustificata dalla necessità di restringere l'ambito operativo dello strumento, al fine di rispettare il principio di proporzionalità e di evitare che si limiti il diritto alla riservatezza e/o alla segretezza delle comunicazioni dell'utente in relazione a fattispecie delittuose ritenute prive di una certa soglia di gravità.

¹¹⁸⁹ Per autorità pubblica si dovrebbe intendere qualsiasi autorità che, in forza del diritto nazionale applicabile, è investito di un mandato per governare o amministrare una parte o un aspetto della vita pubblica, quali i rami del potere giudiziario, legislativo o esecutivo di uno Stato, una provincia o un comune. Cfr., *considerando* n. 34-bis, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

un prestatore di servizi a un'autorità pubblica può essere emesso solo se l'autorità pubblica per la quale i dati sono conservati o trasformati si trova nello Stato di emissione.

Particolare attenzione è dedicata ai casi in cui è richiesta la produzione di dati relativi alle operazioni e al contenuto riferibili a soggetti che l'autorità di emissione ritenga non siano residenti nello Stato di emissione. La disciplina è diversa a seconda che si tratti di dati relativi alle operazioni o al contenuto perché prevede una serie continuata e coordinata di atti differente, in ragione dell'obiettivo da perseguire e del grado di tutela previsto per i diritti fondamentali interessati¹¹⁹⁰.

Andando per ordine, qualora si tratti di dati relativi alle operazioni, l'art. 5, par. 7 della proposta di Regolamento prevede la "consultazione preventiva".

In particolare, qualora l'autorità di emissione abbia ragione di ritenere che il soggetto a cui si riferiscono i dati sia residente al di fuori del proprio territorio e che i dati richiesti siano protetti con immunità e privilegi riconosciuti dal diritto dello Stato di esecuzione, o siano soggetti in tale Stato membro alle norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione¹¹⁹¹, o che la loro divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza e la difesa nazionali, l'autorità di emissione deve chiedere chiarimenti alle autorità competenti dello Stato di esecuzione prima di emettere l'ordine di produzione¹¹⁹². A seguito delle informazioni ottenute, l'autorità di emissione può revocare o adattare l'OEP tenendo conto dei limiti rappresentati come se fossero previsti dal proprio ordinamento¹¹⁹³.

È previsto diversamente per i dati relativi al contenuto. In tale ipotesi, la valutazione relativa alle immunità o ai privilegi avviene in un momento successivo, ossia durante la trasmissione dell'EPOC. Si attiva un meccanismo di notifica di una copia dell'EPOC all'autorità dello Stato di esecuzione nello stesso momento in cui l'EPOC è trasmesso al destinatario.

¹¹⁹⁰ In argomento, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 76.

¹¹⁹¹ Il riferimento è ad esempio agli avvocati, ai ministri di culto o ai giornalisti.

¹¹⁹² In tal senso, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 19; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1349; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 285; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 9.

¹¹⁹³ Ad esempio, se tali privilegi o immunità non sono concessi dal diritto dello Stato membro di emissione, la protezione deve essere adattata, per quanto possibile, al privilegio o all'immunità equivalenti più vicini previsti dal diritto dello Stato membro di emissione, tenuto conto delle finalità e degli interessi perseguiti dalla specifica protezione e degli effetti che ne derivano. Dovrebbero applicarsi le conseguenze giuridiche previste nel proprio diritto nazionale per situazioni analoghe. Al fine di determinare in che modo prendere in considerazione tali motivi come se fossero previsti dal proprio diritto nazionale, l'autorità di emissione può contattare l'autorità notificata per ulteriori informazioni sulla natura e gli effetti della protezione, direttamente o tramite la Rete giudiziaria europea in materia penale o Eurojust. Mentre lo Stato di esecuzione può sollevare una o la totalità delle eccezioni sulla base di tali motivi, la persona i cui dati sono ricercati può solo invocare i propri diritti, quali privilegi o immunità, e non può sollevare obiezioni basate su un interesse fondamentale dello Stato di esecuzione. Cfr., *considerando* n. 35-septies, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

La c.d. *tandem procedure*¹¹⁹⁴, prevista all'art. 7-bis della proposta di Regolamento, prevede che qualora l'autorità di emissione abbia fondati motivi di ritenere che la persona i cui dati sono ricercati non sia residente nel suo territorio, l'autorità di emissione trasmette una copia dell'EPOC all'autorità competente dello Stato di esecuzione nello stesso momento in cui l'EPOC è trasmesso al destinatario¹¹⁹⁵. La notifica non ha effetto sospensivo sugli obblighi del destinatario dell'EPOC. Quanto prima, o comunque entro dieci giorni, l'autorità notificata dovrà informare l'autorità di emissione di qualsiasi circostanza relativa ad immunità, a privilegi, a norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione ovvero a limitazioni necessarie per evitare che la divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza e la difesa nazionali.

Come per la "consultazione preventiva", anche per la *tandem procedure*, a seguito delle informazioni ottenute, l'autorità di emissione può revocare o adattare l'OEP tenendo conto dei limiti rappresentati come se fossero previsti dal proprio ordinamento, ed in caso di revoca, informa immediatamente il destinatario.

Il sistema si chiude con un meccanismo di tutela attivabile successivamente alla produzione dei dati informatici. È possibile che l'autorità di emissione abbia ottenuto dati relativi alle operazioni o al contenuto riferiti a soggetti non residenti nel territorio dello Stato di emissione, nonostante la sussistenza di immunità, privilegi, norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione ovvero limitazioni necessarie per evitare che la divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza e la difesa nazionali.

¹¹⁹⁴ Per tale denominazione, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 77, secondo la quale il meccanismo di notificazione è frutto di un compromesso in sede di negoziato tra gli Stati membri di non facile raggiungimento. In particolare, alla fine del negoziato Finlandia, Germania, Grecia, Lettonia, Repubblica Ceca e Ungheria hanno mantenuto una riserva sul testo di questa norma, ritenendo che dovrebbe essere modificata nel corso del negoziato di trilogia con il Parlamento europeo per estenderne l'applicabilità agli ordini di produzione dei dati relativi alle operazioni e non limitarlo solo ai dati relativi al contenuto e per inserire una previsione finalizzata a consentire all'autorità notificata dello Stato di esecuzione di esercitare un potere di rifiuto dell'ordine di produzione in caso di violazione dei diritti fondamentali. Diversamente, Belgio, Bulgaria, Estonia, Francia, Irlanda, Italia, Polonia, Portogallo e Spagna hanno espresso una riserva sull'introduzione del meccanismo di notificazione previsto all'art. 7-bis ed al meccanismo di "consultazione preventiva" di cui all'art. 5, par. 7 della proposta di Regolamento, ritenendo preferibile l'originaria formulazione della proposta della Commissione europea, che prevede la trasmissione diretta del certificato EPOC al *service provider* senza alcun coinvolgimento dell'autorità competente dello Stato di esecuzione se non nel caso di inadempimento o di opposizione del prestatore di servizi. Infatti, è stato osservato che il valore aggiunto di questa iniziativa legislativa sia da rintracciarsi proprio nella richiesta di acquisizione trasmessa direttamente dall'autorità giudiziaria al *provider*. Una rinuncia in tal senso produrrebbe un meccanismo simile all'ordine europeo di indagine, con il rischio che si riveli inefficiente. La posizione di compromesso raggiunta tra gli Stati membri sul meccanismo di notificazione sopra descritto è stata specularmente recepita nel nuovo articolo 12-bis dell'orientamento generale con riferimento all'utilizzo nel procedimento penale dei dati acquisiti da parte dell'autorità di emissione.

¹¹⁹⁵ Si ritiene che il momento migliore per stabilire se è necessaria la notifica alle autorità dello Stato di esecuzione sia il momento in cui l'ordine è emesso o convalidato. Un successivo cambio di residenza non ha alcun impatto sulla procedura. Cfr., *considerando* n. 35-sexies, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

In tal caso, l'art. 12-*bis* della proposta di Regolamento ha previsto un rimedio *ex post*, che di fatto potrebbe rendere inutilizzabili i dati elettronici ottenuti.

In particolare, qualora all'autorità di emissione sia comunicato che i dati elettronici ottenuti sono protetti, le autorità competenti nello Stato di emissione in possesso delle informazioni devono garantire che durante il procedimento penale tali motivi siano presi in considerazione come se fossero previsti dal proprio diritto nazionale. La disposizione, sebbene vaga, in un'ottica garantista dovrebbe comportare l'inutilizzabilità dei dati elettronici protetti.

Dunque, la persona interessata può far valere i suoi diritti e lo Stato di esecuzione può invocare i propri interessi fondamentali in ogni momento del procedimento penale di cognizione o del procedimento di esecuzione¹¹⁹⁶.

In tutte e tre le ipotesi previste (art. 5, par. 7, art. 7-*bis* e art. 12-*bis* della proposta di Regolamento), quando un privilegio o un'immunità vietino l'uso dei dati ma tali diritti possano essere revocati o qualora l'autorità di emissione intenda usare i dati ottenuti come prova o non ritiri l'ordine nel caso in cui i dati non siano stati acquisiti, lo Stato membro di emissione può richiedere all'autorità interessata la revoca del privilegio o dell'immunità¹¹⁹⁷.

Questo insieme di garanzie è particolarmente rilevante qualora il diritto dello Stato di esecuzione offra una protezione maggiore rispetto al diritto dello Stato di emissione. Il diverso procedimento dedicato ai dati relativi al contenuto rispetto ai dati relativi alle operazioni e il coinvolgimento anticipato dell'autorità dello Stato di esecuzione si spiega perché i dati relativi al contenuto sono di natura particolarmente sensibile, in quanto possono rivelare pensieri ed opinioni delle persone nonché dettagli sensibili della loro vita privata.

Il provvedimento di emissione dell'ordine europeo di produzione contiene i dati relativi all'autorità di emissione e, laddove applicabile, all'autorità di convalida; il destinatario dell'ordine europeo di produzione; l'utente, tranne quando l'unico fine dell'ordine è identificare l'utente, o qualsiasi altro identificativo univoco come il nome utente, l'ID o il nome dell'account per determinare i dati ricercati; la categoria di dati richiesti; se del caso, l'intervallo di tempo per il quale è richiesta la produzione; le disposizioni di diritto penale applicabili dello Stato di emissione; in caso di emergenza o richiesta di divulgazione anticipata, i relativi motivi; se i dati ricercati sono conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società o altra entità diversa da una persona fisica, la conferma che l'ordine è effettuato in conformità al paragrafo 6; i motivi della necessità e della proporzionalità della misura¹¹⁹⁸.

Una volta emesso l'ordine, è necessario compilare il certificato di ordine europeo di produzione (EPOC) in tutte le sue parti, utilizzando il modello in formato standardizzato¹¹⁹⁹. Dunque, anche per l'ordine europeo di produzione, a circolare

¹¹⁹⁶ Cfr., *considerando* n. 35-*sexies*, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹⁹⁷ Cfr., *considerando* n. 35-*octies*, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹¹⁹⁸ Sul contenuto del provvedimento, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1348.

¹¹⁹⁹ In tal senso, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 20.

effettivamente è l'EPOC¹²⁰⁰, un certificato materialmente distinto e diverso dal provvedimento con cui si emette l'OEP¹²⁰¹.

Ai sensi dell'art. 8, par. 3 della proposta di Regolamento, l'EPOC contiene le informazioni presenti del provvedimento dell'ordine europeo di produzione, comprese informazioni sufficienti a permettere al destinatario di identificare e contattare l'autorità di emissione. Tuttavia, sono esclusi i motivi della necessità e della proporzionalità della misura o ulteriori dettagli sulle indagini per evitare che queste ultime possano essere in qualche modo compromesse.

Dopo essere stato firmato, l'EPOC va trasmesso utilizzando canali sicuri che consentano al destinatario la verifica dell'autenticità dell'atto e la certificazione del flusso di comunicazioni, così come avviene per gli ordini europei di conservazione, di cui si è già parlato.

L'EPOC è trasmesso direttamente al rappresentante legale designato dal prestatore di servizi o, in sua assenza, a qualsiasi stabilimento del prestatore di servizi, secondo quanto stabilito dall'art. 7 della proposta di Regolamento¹²⁰².

Qualora i dati ricercati siano conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società o altra entità diversa da una persona fisica¹²⁰³, l'ordine europeo di produzione dovrebbe essere usato solo quando altri atti d'indagine nei confronti della società o dell'ente risultano inappropriati, soprattutto se rischiano di compromettere l'indagine. Questa considerazione è di particolare rilevanza per gli enti di grandi dimensioni, come le società per azioni o gli enti pubblici, che si avvalgono dei servizi di prestatori di servizi per la propria infrastruttura informatica aziendale o i propri servizi informatici aziendali o per entrambi¹²⁰⁴.

Tuttavia, ai sensi dell'art. 5, par. 6 della proposta di Regolamento, qualora i dati ricercati siano conservati o trattati nell'ambito di un'infrastruttura fornita dal prestatore di servizi a una società o altra entità diversa da una persona fisica, e se risulta inappropriato rivolgere atti d'indagine a detta società o entità, soprattutto perché si rischierebbe di compromettere l'indagine, ad esempio perché si sospetta che la società o l'ente possa essere coinvolto nel caso di specie o vi sono indizi di collusione con il

¹²⁰⁰ Così, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 285.

¹²⁰¹ In tal senso, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 174.

¹²⁰² Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1350; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 284; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 174. V., inoltre, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 79, secondo la quale si tratterebbe di una ipotesi di riserva «finalizzata a garantire la tenuta del sistema qualora il prestatore di servizi non abbia (ancora) nominato il proprio rappresentante perché la Direttiva non è stata ancora recepita dagli Stati membri e dunque non ha l'obbligo giuridico di farlo, oppure perché tale obbligo non gli si applica in quanto è stabilito od opera solo in uno Stato membro».

¹²⁰³ Di solito, si tratta dei servizi di *hosting*.

¹²⁰⁴ In tali situazioni il primo destinatario dell'ordine europeo di produzione dovrebbe essere la società o altro ente. Tale società o altro ente potrebbe non essere un prestatore di servizi rientrante nell'ambito di applicazione del Regolamento.

soggetto sottoposto all'indagine, l'ordine europeo di produzione è rivolto solo al prestatore di servizi¹²⁰⁵.

Con la ricezione dell'EPOC da parte del destinatario si apre la fase di esecuzione, nella quale la serie continuata e coordinata di atti è volta, generalmente, a far acquisire, quale risultato finale, i dati elettronici richiesti all'autorità di emissione.

L'esecuzione dell'ordine deve avvenire tempestivamente ed in termini obbligatori¹²⁰⁶, mentre la trasmissione dei dati deve avvenire secondo modalità sicure e affidabili¹²⁰⁷. Il termine previsto dall'art. 9 della proposta di Regolamento è di dieci giorni dalla ricezione del certificato. Tuttavia, l'autorità di emissione, previa indicazione dei motivi¹²⁰⁸, può specificare un termine inferiore nel caso di trasmissione anticipata. Dalla trasmissione anticipata va distinta l'esecuzione di emergenza¹²⁰⁹, prevista all'art. 9, par. 2 della proposta di Regolamento, secondo cui i dati richiesti debbano essere prodotti senza indebito ritardo e comunque non oltre il termine stringente di sei ore dalla ricezione dell'EPOC¹²¹⁰.

È evidente che il maggior vantaggio dell'OEP sia relativo alla breve durata del procedimento, o meglio dell'esecuzione relativa alla produzione dei dati elettronici, basato sul principio della massima efficienza e di minore rischio di dispersione del dato digitale¹²¹¹. Invero, ove riuscisse a funzionare al massimo delle potenzialità, lo strumento consentirebbe di ottenere dati elettronici in pochi giorni o ore¹²¹², nel rispetto dei diritti fondamentali, con un impatto dirompente sulle investigazioni digitali.

Sia la trasmissione anticipata sia l'esecuzione di emergenza vanno tenute distinte dall'emissione d'urgenza, innanzitutto perché le finalità sono diverse, così come sono diverse le attività, ma anche perché l'emissione d'urgenza è attività possibile nella fase precedente.

¹²⁰⁵ In argomento, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1349.

¹²⁰⁶ Sul punto, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 286; F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, cit., 1 ss.

¹²⁰⁷ L'art. 9, par. 1 della proposta di Regolamento recita «Quando riceve l'EPOC il destinatario provvede affinché i dati richiesti siano trasmessi direttamente, secondo modalità sicure e affidabili che consentano di stabilire l'autenticità e l'integrità del certificato, all'autorità di emissione o alle autorità di contrasto». Ebbene, il riferimento, più che al certificato, dovrebbe essere ai dati che sono trasferiti.

¹²⁰⁸ Il certificato EPOC prevede quali motivi, a titolo esemplificativo, il pericolo imminente che i dati richiesti siano cancellati, la necessità di eseguire un altro atto d'indagine urgente che non può essere condotto senza i dati mancanti o ne dipende in altro modo, l'imminenza della data del processo, la sottoposizione dell'indagato o imputato a custodia cautelare. È poi lasciato spazio ad altre motivazioni che l'autorità di emissione può liberamente indicare.

¹²⁰⁹ Secondo quanto indicato nel certificato EPOC, i casi di emergenza riguarderebbero una minaccia imminente per la vita o l'integrità fisica di una persona. La formulazione sembrerebbe ricalcare i presupposti previsti per la cooperazione accelerata nel Secondo protocollo alla convenzione sulla criminalità informatica.

¹²¹⁰ In dottrina vi è chi ha ritenuto il termine di sei ore troppo breve per rispondere agli ordini, soprattutto se si considerano le realtà meno strutturate che potrebbero non essere in grado di rispettare le tempistiche. Cfr., O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 20.

¹²¹¹ Sul punto, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2724.

¹²¹² Così, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 286.

Con l'emissione d'urgenza l'autorità può attivare sia la trasmissione anticipata sia l'esecuzione di emergenza. Tuttavia, le due ipotesi di esecuzione accelerata non presuppongono obbligatoriamente che in fase di emissione sia stata adottata la procedura d'urgenza, essendo richiedibili anche nelle ipotesi di emissione ordinaria.

In caso di una richiesta di esecuzione di emergenza non ottemperata da parte del rappresentante legale, ai sensi dell'art. 6, par. 3 della proposta di Regolamento, l'ordine europeo di produzione può essere rivolto a qualsiasi stabilimento del prestatore di servizi nell'Unione. Analogamente, ciò avviene quando il rappresentante legale sia inadempiente agli obblighi dell'ordine europeo di produzione di cui all'art. 9 della proposta di Regolamento e l'autorità di emissione ritenga che sussista un grave rischio di perdita dei dati¹²¹³.

L'esecuzione dell'ordine di produzione non è certo automatica e sempre possibile. Vi sono alcune zone d'ombra in cui possono annidarsi elementi di incertezza che rendono in quello specifico lasso temporale o sempre ineseguibile l'ordine. Si tratta di tre ipotesi previste dall'art. 9, parr. 3, 4 e 5 della proposta di Regolamento.

Nel primo caso, l'EOP potrebbe essere incompleto o contenere errori o avere informazioni insufficienti per l'esecuzione. Di fronte ad un certificato simile, il destinatario deve avviare un dialogo con l'autorità di emissione chiedendo chiarimenti senza indebito ritardo usando il relativo modulo in cui inserire le informazioni sull'impossibilità di eseguire l'EPOC ed informando l'autorità di emissione se è stato possibile o meno procedere all'identificazione e alla conservazione dei dati. Entro cinque giorni, l'autorità di emissione risponde revocando o modificando o inviando i chiarimenti necessari¹²¹⁴. Dunque, l'autorità di emissione ha la possibilità di rettificare o riesaminare l'EPOC in una fase precoce, prima di attivarsi per far rispettare l'ordine.

Il destinatario deve informare l'autorità di emissione anche qualora non possa fornire i dati a causa di forza maggiore o per impossibilità materiale non imputabile al rappresentante né al prestatore di servizi, ad esempio quando la persona i cui dati sono richiesti non era cliente del servizio o quando i dati sono stati legittimamente cancellati dal prestatore di servizi, ad esempio nell'ambito di altri obblighi di tutela della vita privata, prima che il prestatore o il suo rappresentante legale ricevesse l'ordine. L'autorità di emissione deve conoscere tali circostanze per reagire velocemente, provando ad acquisire i dati elettronici da un altro prestatore o provvedendo al ritiro dell'ordine laddove ciò non abbia senso¹²¹⁵.

Terza ipotesi è prevista all'art. 9, par. 5 della proposta di Regolamento. In tutti i casi in cui per motivi diversi da quelli sinora illustrati¹²¹⁶ il destinatario non fornisce le

¹²¹³ In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 79 ss.

¹²¹⁴ Cfr., R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1351; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 80; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 174.

¹²¹⁵ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1351.

¹²¹⁶ Ad esempio, si potrebbe trattare di ipotesi in cui ad emettere l'ordine di produzione non sia stata un'autorità di convalida o un'autorità di emissione individuata ai sensi dell'art. 4 della proposta di Regolamento ovvero l'ordine di produzione avente ad oggetto i dati relativi alle operazioni o al contenuto

informazioni o non le fornisce in maniera esaustiva o entro i termini, è necessario informare dei motivi l'autorità di emissione senza indebito ritardo mediante il modulo relativo alle informazioni sull'impossibilità di eseguire.

Una volta che l'autorità di emissione sia venuta a conoscenza dei motivi di ineseguibilità, è possibile bloccare l'esecuzione e rivalutare la strategia investigativa. Infatti, l'autorità di emissione potrebbe ritirare l'ordine di conservazione qualora ritenga esaustive le motivazioni del destinatario. Altrimenti, ai sensi dell'art. 7, par. 4 della proposta di Regolamento, se ha indirizzato l'EPOC ad un rappresentante legale e ritenga che questi non abbia ottemperato agli obblighi, può rivolgere l'OEC a qualsiasi stabilimento del prestatore di servizi nell'Unione, se sussiste un grave rischio di perdita dei dati ovvero potrebbe attivare la procedura prevista all'art. 14 della proposta di Regolamento, con cui si instaura un procedimento simile a quello previsto per l'ordine europeo di indagine.

Se i dati non sono prodotti immediatamente, in particolare quando è avviato un dialogo tra il destinatario e l'autorità di emissione, con conseguente inosservanza dei termini di cui all'art. 9 della proposta di Regolamento, il prestatore di servizi deve conservare, in via cautelativa, i dati per evitare che questi vengano persi, tranne se le informazioni contenute nell'EPOC non consentono di identificarli. In tal caso il destinatario chiede chiarimenti conformemente al par. 3.

La conservazione può servire per un successivo EPOC chiarito o un ordine europeo di indagine o una successiva richiesta di assistenza giudiziaria. Ovviamente, se la produzione e la conservazione dei dati non sono più necessarie, l'autorità di emissione ne informa il destinatario senza indebito ritardo¹²¹⁷.

Orbene, in queste tre ipotesi la procedura può subire un ritardo, in ragione degli imprevisti generatisi. Pertanto, appare opportuno ritenere che i termini per la produzione dei dati elettronici decorrano dal momento in cui sarà poi possibile produrre i dati, qualora l'ordine non sia stato ritirato.

7.1. (Segue). *La procedura di riesame in caso di contrasto con il diritto di un Paese terzo*

Tra i motivi diversi che il destinatario potrebbe addurre, ai sensi dell'art. 9, par. 5, della proposta di Regolamento, vi è il contrasto con il diritto applicabile di un Paese terzo. Invero, una volta ricevuto l'EPOC, il destinatario potrebbe rilevare degli obblighi contrastanti con il Paese terzo in cui ha sede il prestatore di servizi.

Per cui, in conformità a quanto stabilito dalle norme sull'esecuzione dell'OEP, è tenuto ad inviare all'autorità di emissione il modulo contenente le informazioni relative all'impossibilità di eseguire l'EPOC, con il quale comunica che ottemperare all'ordine europeo di produzione contrasterebbe con il diritto applicabile di un Paese terzo.

non sia stato emesso per uno dei reati di cui all'art. 5, par. 4 della proposta di Regolamento oppure il servizio non è coperto dalla proposta di Regolamento.

¹²¹⁷ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1351 ss.

Si tratta di un atto di non poco conto, perché attiva la procedura di cui all'art. 16, della proposta di Regolamento¹²¹⁸, con il quale si procede al riesame dell'ordine di produzione¹²¹⁹ alla luce dell'obbligo confliggente invocato dal *service provider*¹²²⁰.

La procedura può avere avvio solo a seguito del rifiuto del destinatario alla produzione dei dati elettronici richiesti perché ostano norme di divieto di uno Stato terzo al cui rispetto è tenuto. In particolare, il modulo contenente le informazioni relative all'impossibilità di eseguire l'EPOC assume la forma dell'"opposizione motivata".

Infatti, nell'informare l'autorità di emissione, il destinatario deve compilare il modulo indicando tutte le informazioni pertinenti sul diritto del Paese terzo, sulla sua applicabilità al caso di specie e sulla natura dell'obbligo contrastante, secondo le modalità di cui all'art. 9, par. 5 e 6, della proposta di Regolamento, con i quali si prevede la notificazione dell'intenzione di non ottemperare all'EPOC¹²²¹ e la contestuale conservazione dei dati, ove possibile¹²²².

¹²¹⁸ In principio, erano state previste due procedure differenti a seconda che il divieto di consegna dei dati fosse volto alla tutela di diritti fondamentali dell'individuo o di interessi fondamentali del Paese terzo (articolo 15), ovvero tutelasse interessi di natura diversa (articolo 16). Nello specifico, l'impianto originario della proposta normativa prevedeva all'art. 15 che, qualora l'ottemperanza all'ordine di produzione determinasse la violazione della legislazione di uno Stato terzo finalizzata alla tutela dei diritti fondamentali delle persone interessate o degli interessi fondamentali del Paese terzo connessi alla sicurezza o alla difesa nazionali, il rappresentante legale del *service provider* potesse attivare una procedura innanzi alla competente autorità giurisdizionale dello Stato di emissione. La valutazione di merito sulla normativa dello Stato terzo era volta a verificare se il diritto del Paese terzo, anziché tutelare i diritti fondamentali o interessi fondamentali dello Stato connessi alla sicurezza o alla difesa nazionali, intendesse manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali. Qualora all'esito del riesame l'autorità giurisdizionale dello Stato di emissione avesse ritenuto che non sussistesse alcun contrasto, l'organo giurisdizionale avrebbe dovuto avviare una consultazione obbligatoria con lo Stato terzo, il cui eventuale parere negativo avrebbe dispiegato un effetto ostativo vincolante per lo Stato procedente. Nel corso del negoziato, la norma ha destato molte perplessità, poiché attribuiva al prestatore di servizi un singolare ruolo di garante degli interessi politici dello Stato terzo, conferendogli di fatto il potere di bloccare, anche se solo temporaneamente, l'esecuzione di un ordine. Inoltre, la procedura appariva macchinosa e lenta, incompatibile con le specifiche caratteristiche del dato elettronico. La valutazione di tali circostanze ha comportato l'eliminazione della doppia procedura dall'orientamento generale. Per una ricostruzione della precedente versione normativa, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1290; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 287 ss.; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 82; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 9.

¹²¹⁹ Un mezzo di ricorso analogo non è previsto anche per l'ordine europeo di conservazione. Probabilmente la scelta è dovuta al fatto che l'ordine di conservazione non comporta di per sé la divulgazione dei dati e non crea particolari gravi rischi di lesione ai diritti, così come l'ordine europeo di produzione.

¹²²⁰ In tal senso, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 81.

¹²²¹ Così, E. COLOMBO, *Ordini europei di produzione e di conservazione di prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, cit., p. 2727; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 82.

¹²²² Cfr., considerando n. 53, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

Tra gli obblighi contrastanti, sono esclusi l'assenza – nel diritto applicabile del Paese terzo – di disposizioni analoghe riguardo alle condizioni, alle formalità e alle procedure di emissione di un ordine di produzione, nonché la sola circostanza che i dati sono conservati in un Paese terzo¹²²³.

Più nello specifico, per rendere più agevole l'attività di riesame che dovrà compiere l'autorità di emissione, nel modulo dovranno essere indicati il titolo della legge o delle leggi del Paese terzo che si adduce essere in contrasto; le disposizioni di legge applicabili e il testo delle disposizioni pertinenti; la natura dell'obbligo contrastante, compreso l'interesse tutelato dal diritto del Paese terzo, precisando se si tratta di diritti fondamentali delle persone fisiche o di interessi fondamentali del Paese terzo connessi alla sicurezza e alla difesa nazionali ovvero di altri interessi, ed indicando quali siano; le motivazioni che hanno spinto il privato a ritenere perché la legge indicata sia applicabile al caso di specie, perché sussista un contrasto con il caso di specie e quale sia il collegamento tra il prestatore di servizi e il Paese terzo in questione. Il modulo dovrà, inoltre, indicare le possibili conseguenze per il destinatario in caso di ottemperanza all'ordine europeo di produzione, comprese le sanzioni in cui può incorrere.

L'invio del modulo contenente l'opposizione motivata attiva la procedura di riesame, un mezzo di ricorso avente lo scopo di tutelare i diritti dei singoli e la cortesia internazionale e, più precisamente, il diritto di un Paese terzo che vieta la divulgazione dei dati per la necessità di tutelare i diritti fondamentali o gli interessi preminenti, come la sicurezza o la difesa nazionali¹²²⁴. Il modulo è presentato al più tardi dieci giorni dopo la data in cui il destinatario ha ricevuto l'EPOC.

Lo strumento è stato creato perché in una procedura *in rem* simile, oltre alle persone i cui dati sono richiesti, anche il prestatore di servizi e i Paesi terzi possono essere interessati dall'atto d'indagine¹²²⁵. Pertanto, è stato previsto un meccanismo specifico di riesame giurisdizionale nel caso in cui ottemperare all'ordine europeo di produzione costringa il destinatario a violare un obbligo giuridico di un Paese terzo¹²²⁶.

In tal modo, non si è voluto – a ragione – riconoscere in capo al prestatore di servizi un potere decisorio definitivo relativo all'esecuzione di un ordine di produzione, bensì si è riconosciuto un "diritto ad opporsi, per riesaminare".

Sicuramente la procedura che vi consegue appesantisce il meccanismo di produzione dei dati, ma al contempo favorisce la tutela dei diritti fondamentali ed i rapporti con gli Stati terzi, sino a rappresentare una forma di stimolo nei confronti di questi ultimi ad innalzare il proprio livello di garanzie¹²²⁷.

¹²²³ Cfr., art. 16, par. 2 della proposta di Regolamento.

¹²²⁴ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 24; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1353; A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione europea: le Proposte della Commissione europea sugli ordini di produzione e conservazione di prove elettroniche (e-evidence)*, cit., p. 9; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 176.

¹²²⁵ Così, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1353.

¹²²⁶ Cfr., considerando n. 47, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹²²⁷ Vi è chi ha inoltre sostenuto che il mezzo di ricorso rappresenta «un ulteriore livello di controllo che è volto a salvaguardare direttamente e immediatamente gli interessi sottesi alla facoltà di opposizione (diritti fondamentali e interessi nazionali), ma indirettamente e mediamente quell'interesse alla *comity* tra

Con il recepimento dell'opposizione motivata si apre la procedura di riesame. La procedura di riesame si divide in due subprocedimenti. In un primo subprocedimento, l'autorità di emissione riesamina l'ordine sulla base di quanto indicato nell'obiezione motivata, tenendo conto degli stessi criteri che dovrà eventualmente seguire l'organo giurisdizionale competente per il riesame¹²²⁸.

Se decide di ritirare l'ordine, la procedura si conclude, se invece intende confermarlo, richiede il riesame ed invia gli atti all'organo giurisdizionale competente del proprio Stato membro, attivando così il secondo subprocedimento. L'esecuzione dell'ordine europeo di produzione è sospesa sino alla conclusione della procedura di riesame.

In dottrina ci si è chiesto chi possa essere in Italia l'organo giurisdizionale competente. Vi è chi ritiene possibile che sia lo stesso organo o potrebbe esservi un deferimento *ex officio* ad altra sezione, all'organo superiore o al presidente dello stesso¹²²⁹.

Pur riconoscendo la difficoltà di una risposta soddisfacente e l'imprescindibile necessità di una normativa interna che dovrà indicarne la competenza, è possibile individuare alcune coordinate e principi per ricondurre tutto a sistema.

Innanzitutto, l'art. 9, par. 3, della proposta di Regolamento, richiede che sia individuato un organo giurisdizionale, per cui sembrerebbe già da escludere l'ufficio del pubblico ministero. Siccome un ordine di produzione può essere emesso in qualsiasi fase del procedimento di cognizione, dovrebbe escludersi anche la competenza in capo al giudice per le indagini preliminari. In un'ottica garantista, che tuteli anche la difficoltà di un accertamento che potrà far ricorso anche a personalità esterne in possesso di specifiche conoscenze relative al diritto dello Stato estero, si potrebbe individuare la competenza in un organo collegiale come il tribunale del riesame o la Corte d'Appello.

È possibile dividere il riesame dell'organo giurisdizionale in due fasi: fase di valutazione e fase di decisione.

Va preliminarmente chiarito che l'organo giurisdizionale, nell'adempire all'ufficio, può basarsi, se necessario, su appropriate competenze esterne¹²³⁰. In particolare, per pareri provenienti da competenze esterne, si può far riferimento sia alle informazioni richieste all'autorità competente del Paese terzo, ella misura in cui ciò non ostacoli il procedimento penale, in applicazione dell'art. 16, par. 5-ter, della proposta di Regolamento, sia a pareri di esperti, ove disponibili, relativi all'interpretazione del diritto del Paese terzo¹²³¹.

le autorità di Paesi europei e di paesi non europei che si colloca alla base degli attuali disegni di riforma, imponendo di ridurre al minimo i rischi di conflitto tra ordinamenti». Sul punto, O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss.

¹²²⁸ Cfr., *considerando* n. 48, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹²²⁹ In tal senso, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 24.

¹²³⁰ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1353; R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 83.

¹²³¹ Per agevolare la circolazione delle informazioni, l'efficienza delle procedure e l'economia processuale, si è pensato di far beneficiare gli organi giurisdizionali delle esperienze acquisite da altri organi giurisdizionali sulla stessa questione o su questioni simili creando una apposita sezione dedicata su una piattaforma centrale quale il progetto SIRIUS e/o la Rete giudiziaria europea. In tal modo, si renderebbero disponibili le informazioni e la giurisprudenza relative all'interpretazione del diritto dei Paesi terzi e alle procedure di conflitto degli Stati membri. Cfr., *considerando* n. 50, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

Dunque, la consultazione con le autorità del Paese terzo non avrebbe un carattere obbligatorio e vincolante, come pur era previsto nella prima stesura della proposta originaria di Regolamento¹²³².

In fase di valutazione, l'organo giurisdizionale è chiamato a valutare se sussista un contrasto. Nello specifico, in ordine logico, dovrà dapprima esaminare se, in base alle circostanze del caso concreto, si applica il diritto del Paese terzo. In caso negativo, la procedura si conclude e l'OEP è confermato, in caso affermativo, l'organo giurisdizionale dovrà chiarire se il diritto del Paese terzo, ove applicato alle circostanze specifiche del caso, vieta la divulgazione dei dati elettronici richiesti. Nel caso in cui non ravvisi tale contrasto, l'organo giurisdizionale conferma l'ordine, altrimenti si passa alla fase di decisione.

Nella fase di decisione, appurata la sussistenza del contrasto, l'organo giurisdizionale è chiamato a decidere se confermare o revocare l'ordine, sulla base di due insiemi di criteri. Un primo insieme di criteri è di particolare rilievo e nella valutazione ponderata avranno un peso specifico maggiore e saranno valutati con preminenza. Si tratta del criterio di valutazione attinente: all'interesse tutelato dal diritto del Paese terzo, compresi i diritti fondamentali e altri interessi che impediscono la divulgazione dei dati, in particolare gli interessi di sicurezza nazionale del Paese terzo¹²³³; alla solidità del collegamento tra le due giurisdizioni coinvolte, valutata in base all'ubicazione, alla cittadinanza e alla residenza della persona i cui dati sono richiesti e/o della vittima ed in base al luogo in cui il reato in questione è stato commesso¹²³⁴.

Del secondo insieme fanno, invece, parte il criterio relativo: al grado di collegamento tra il prestatore di servizi e il Paese terzo in questione¹²³⁵; all'interesse dello Stato dell'indagine a ottenere le prove in questione, sulla base della gravità del reato e dell'importanza di acquisire le prove rapidamente; alle possibili conseguenze per il destinatario o il prestatore di servizi in caso di ottemperanza all'OEP, comprese le sanzioni in cui può incorrere¹²³⁶.

La valutazione compiuta è basata sul bilanciamento degli interessi a favore e contro la conferma dell'ordine, valutando quali interessi preminenti quelli appartenenti al primo insieme¹²³⁷.

L'organo giurisdizionale può decidere se revocare o confermare l'ordine. Se revoca l'ordine, informa l'autorità di emissione e il destinatario. In tal caso, nulla esclude che possa essere emesso un ordine di conservazione per consentire all'autorità di emissione di chiedere la produzione dei dati elettronici attraverso altri canali, come l'assistenza

¹²³² Così, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 83.

¹²³³ Questo criterio sarebbe proiettato a verificare se la normativa dello Stato terzo è finalizzata anziché a tutelare i diritti fondamentali o gli interessi del Paese terzo connessi alla sicurezza o alla difesa, a proteggere altri interessi o attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali.

¹²³⁴ Cfr., *considerando* n. 48, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹²³⁵ In tale contesto, il luogo di conservazione dei dati non è di per sé sufficiente per stabilire un grado di collegamento significativo

¹²³⁶ Sul punto, R. PEZZUTO, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, cit., p. 83.

¹²³⁷ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1354 ss.; S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 176.

giudiziaria o la cortesia istituzionale¹²³⁸. Se intende confermare, informa l'autorità di emissione ed il destinatario, che deve procedere ad eseguire l'ordine.

Orbene, l'istituto apporta una grande innovazione nel mondo del diritto e della cooperazione giudiziaria in materia penale perché l'opposizione da parte del destinatario è rivolta all'autorità di emissione e non ad una autorità dello Stato di esecuzione. In questo senso, la proposta si sgancia dal tradizionale principio di territorialità, che collega la giurisdizione al luogo in cui i dati sono conservati¹²³⁹.

Invero, sembra che solo in assenza della collaborazione del destinatario il procedimento venga nuovamente affidato alle autorità competenti degli Stati membri¹²⁴⁰, secondo le regole di cui all'art. 14 della proposta di Regolamento.

Questo approccio tiene conto dei recenti sviluppi tecnologici, come ad esempio il *cloud computing* e dell'impraticabilità delle classiche soluzioni basate sul principio della territorialità ed appare in linea con i recenti sviluppi in tema di ricerca e formazione della prova elettronica transnazionale presenti sia nel Secondo protocollo alla Convenzione sulla criminalità informatica, sia nel CLOUD Act Statunitense.

8. L'intervento dell'autorità di esecuzione in caso di inottemperanza

Il destinatario degli ordini europei di produzione e degli ordini europei di conservazione non può e non deve mai essere attore decisionale di ultima istanza, perché pur sempre portatore di interessi privatistici, anche a carattere economico. In quanto tale, non può essere e non può apparire un soggetto terzo ed imparziale¹²⁴¹.

La funzione di garanzia e di controllo, che necessariamente deve essere assicurata in procedimenti delicati quali quelli previsti per l'ordine europeo di conservazione e per l'ordine europeo di produzione, consiglia di individuare in un'autorità giudiziaria – e meglio ancora in un'autorità giurisdizionale – l'organo che possa legalmente verificare eventuali inottemperanze del destinatario o conflitti tra l'autorità di emissione ed il destinatario.

Nell'alveo di tale teoria generale si inserisce la scelta del legislatore europeo di individuare una procedura di esecuzione in caso di inottemperanza del destinatario in cui

¹²³⁸ Cfr., *considerando* n. 53, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹²³⁹ In tal senso, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 176.

¹²⁴⁰ In tal senso, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 436.

¹²⁴¹ È nota in dottrina la distinzione tra soggetto e parte del processo. Sono soggetti i titolari di poteri di iniziativa nel procedimento, mentre sono parti coloro che siano portatori di un interesse all'interno del processo, come ad esempio colui che ha chiesto una decisione o colui contro cui è stata chiesta una decisione. Chi si fa portatore di un interesse non appare equidistante o nei confronti delle altre parti o nei confronti dell'oggetto del procedimento o in relazione ad entrambe le circostanze e, pertanto, non può essere né apparire imparziale. Sui concetti, in dottrina, *ex multis*, G. BELLAVISTA, *Lezioni di diritto processuale penale* (a cura di G. TRANCHINA), Milano, 1979, p. 181; A.A. DALIA, M. FERRAIOLI, *Manuale di diritto processuale penale*, cit., p. 113 ss.; P. FERRUA, *Il "giusto processo" in Costituzione*, in *Dir. giust.*, 1, 2000, p. 78; G. LEONE, *Trattato di diritto processuale penale*, I, Napoli, 1961, p. 248 secondo cui parte «è colui che tende ad una decisione giudiziale di fronte ad un altro soggetto, ed è colui di fronte a cui tale decisione viene chiesta»; P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 66 ss.

è coinvolta l'autorità competente dello Stato di esecuzione¹²⁴², che instaura il consueto dialogo ed il rapporto diretto tra autorità di emissione ed autorità di esecuzione, come classicamente avviene nelle procedure basate sul principio del mutuo riconoscimento¹²⁴³.

La procedura prova a rintracciare un equilibrio tra le esigenze di celerità – imprescindibile quando ad oggetto si hanno elementi elettronici – e le esigenze di tutela dei diritti fondamentali dei singoli, degli interessi collettivi e preminenti di uno Stato quale la sicurezza e la difesa nazionale. Nel tentare un bilanciamento, il legislatore europeo ha creato una procedura all'evidenza del tutto simile a quella prevista per il riconoscimento dell'ordine europeo di indagine, ma rispetto ad essa più rapida.

Nello specifico, l'art. 14 introduce anche una procedura aggravata a seguito di inottemperanza per far eseguire gli ordini con l'aiuto dello Stato membro in cui è situato il destinatario del certificato trasmesso¹²⁴⁴.

I presupposti della procedura si individuano in elementi afferenti alla stasi del procedimento e/o all'inerzia del destinatario, il quale non ottempera all'EPOC-PR o all'EPOC nel termine previsto, senza fornire motivi o fornendo motivi ritenuti irricevibili da parte dell'autorità di emissione.

La procedura è attivata dall'autorità di emissione e prevede l'intervento dell'autorità di esecuzione¹²⁴⁵ stabilita sul territorio dello Stato di esecuzione. In particolare, valutati i presupposti, l'autorità di emissione richiede che sia applicata la procedura di cui all'art. 14, inviando all'autorità di esecuzione l'OEP e l'EPOC ovvero l'OEC e l'EPOC-PR, unitamente al modulo contenente le informazioni relative all'impossibilità di eseguire di cui all'allegato III della proposta di Regolamento e a qualsiasi altro documento ritenuto pertinente ai fini dell'esecuzione dell'ordine.

L'autorità di emissione deve trasmettere l'intero ordine, comprensivo dei motivi che accertino la necessità e la proporzionalità, per consentire un attento vaglio basato su un'analisi globale dei documenti e delle circostanze che hanno indotto l'autorità di emissione ad emettere la decisione e il privato a non ottemperare.

Ricevuta la documentazione, senza indebito ritardo e comunque nel termine di non oltre cinque giorni lavorativi dalla ricezione dell'ordine, l'autorità di esecuzione deve procedere al riconoscimento ovvero al rigetto dell'ordine¹²⁴⁶, compiendo una valutazione

¹²⁴² Ai sensi dell'art. 2, n. 13 della proposta di Regolamento, lo Stato di esecuzione è individuato in relazione al luogo in cui risiede o è stabilito il destinatario dell'OEP o dell'OEC.

¹²⁴³ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1352.

¹²⁴⁴ Sulle procedure di modifica previste all'art. 14 della proposta di Regolamento, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 21 ss., secondo cui si dovrebbe più correttamente parlare di procedura di "esecuzione coatta"; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1352 ss.; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 287.

¹²⁴⁵ L'indicazione della specifica autorità di esecuzione competente a ricevere, riconoscere e far eseguire l'ordine è evidentemente demandata ai singoli Stati membri, i quali, con un atto legislativo interno, dovranno indicare l'autorità competente e comunicarlo agli organismi europei della cooperazione giudiziaria in materia penale. Sarebbe opportuno che, come avvenuto per l'ordine europeo di indagine, anche per gli ordini europei di conservazione e di produzione si proceda ad inserire le autorità di esecuzione competenti in una apposita sezione del sito della Rete giudiziaria europea. La comunicazione dovrebbe avvenire anche ad Eurojust, in modo tale da consentire a quest'ultima un'effettiva attività di coordinamento anche in relazione ai nuovi strumenti per la ricerca della prova elettronica.

¹²⁴⁶ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 22.

volta ad individuare l'inesistenza di motivi di rifiuto¹²⁴⁷, previa consultazione dell'autorità di emissione.

Sono motivi di rifiuto di un ordine di produzione e, in quanto tali, non consentono il riconoscimento o l'esecuzione di un ordine europeo di produzione: l'emissione o la convalida dell'ordine da parte di un'autorità non legittimata ai sensi dell'art. 4 della proposta di Regolamento; l'emissione di un OEP per un reato non compreso nell'elenco dei reati-presupposto di cui all'art. 5, par. 4 della proposta di Regolamento e per cui non è possibile richiedere un ordine; l'impossibilità materiale all'esecuzione da parte del destinatario o la presenza di errori manifesti nell'EPOC; l'impossibilità alla produzione dei dati richiesti perché questi non sono conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC; la non riconducibilità del servizio nell'ambito di applicazione del Regolamento; l'esistenza di un privilegio, di una immunità, di norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione ovvero di limitazioni necessarie per evitare che la divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza e la difesa nazionali¹²⁴⁸.

Invece, sono motivi di rifiuto dell'ordine europeo di conservazione: l'emissione o la convalida dell'ordine da parte di un'autorità non legittimata ai sensi dell'art. 4 della proposta di Regolamento; l'impossibilità materiale all'esecuzione da parte del destinatario o la presenza di errori manifesti nell'EPOC-PR; l'impossibilità alla produzione dei dati richiesti perché questi non sono conservati dal prestatore di servizi o per suo conto al momento della ricezione dell'EPOC-PR; la non riconducibilità del servizio nell'ambito di applicazione del Regolamento.

Accertata l'insussistenza di un motivo di rifiuto, l'autorità di esecuzione riconosce l'ordine ed emette un provvedimento con il quale ingiunge formalmente al destinatario di ottemperare all'obbligo pertinente¹²⁴⁹, fissando un termine per l'ottemperanza o per l'opposizione. L'art. 14, par. 3, della proposta di Regolamento, non individua un termine preciso perché evidentemente lascia al prudente apprezzamento dei legislatori nazionali l'indicazione di un lasso temporale entro cui procedere.

Al provvedimento è allegata un'informativa relativa alla possibilità per il destinatario di opporsi all'esecuzione invocando uno dei motivi di rifiuto¹²⁵⁰ e delle sanzioni applicabili in caso di inottemperanza.

¹²⁴⁷ Alcuni motivi di rifiuto hanno un carattere perlopiù formalistico-procedurale, altri più un carattere sostanziale. Sul punto O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss. Inoltre, vi è stata una sensibile riduzione dei motivi di rifiuto rispetto all'ordine europeo di indagine, il che dovrebbe indicare una maggior apertura verso una nuova e conquistata fiducia reciproca.

¹²⁴⁸ Siccome alla procedura si applica per analogia l'art. 5, par. 8 della proposta di Regolamento, qualora sia rilevata l'esistenza di un privilegio o di una immunità, previa richiesta da parte dell'autorità competente dello Stato di emissione, l'autorità di esecuzione può chiedere all'autorità competente dello Stato di esecuzione di esercitare il potere di revoca. Qualora, invece, la revoca spetti ad una autorità di un altro Stato membro o di un Paese terzo o a una organizzazione internazionale, l'autorità di emissione può chiedere all'autorità interessata di esercitare il suo potere di revoca.

¹²⁴⁹ In tal senso, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1352.

¹²⁵⁰ Ad eccezione dell'esistenza di un privilegio, di una immunità, di norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione ovvero di limitazioni necessarie per evitare che la divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza e la difesa nazionali.

Ricevuto il provvedimento di ingiunzione, il destinatario può – nei termini indicati – eseguire l'ordine e trasmettere i dati all'autorità di esecuzione ovvero avanzare un'opposizione sulla base di limitati e tassativamente determinati motivi¹²⁵¹.

Il procedimento di opposizione al provvedimento di ingiunzione¹²⁵² assume tutte le caratteristiche di un mezzo di ricorso in cui è garantito il principio del contraddittorio. La proposta di Regolamento individua la competenza in capo all'autorità di esecuzione, lasciando anche in questo caso ai singoli legislatori nazionali la possibilità di indicare l'autorità specifica.

Tuttavia, ragioni di opportunità, dettate dal rispetto dei principi fondamentali e, più specificamente, del principio di imparzialità, terzietà e legalità, indurrebbero a ritenere che l'autorità di esecuzione da adire dovrebbe essere diversa dall'autorità di esecuzione che ha provveduto al riconoscimento. Ciò sarebbe in linea anche con quanto stabilito in tema di impugnazioni dell'ordine europeo di indagine.

Invero, ai sensi dell'art. 13, comma 1, d.lgs. 21 giugno 2017, n. 108, per la procedura passiva, in caso di richiesta dall'estero, qualora sia impugnato il decreto di riconoscimento, i legittimati possono proporre opposizione al giudice per le indagini preliminari, autorità evidentemente diversa da quella che generalmente è legittimata al riconoscimento, ossia l'ufficio del pubblico ministero.

L'opposizione contiene uno dei motivi previsti tra i motivi di rifiuto, ad eccezione di quelli relativi all'esistenza di un privilegio, di una immunità, di norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione ovvero di limitazioni necessarie per evitare che la divulgazione possa incidere su interessi fondamentali dello Stato di esecuzione come la sicurezza e la difesa nazionali.

Nel rispetto del principio del contraddittorio, il procedimento di opposizione consente all'autorità di esecuzione di richiedere, se necessario, delle informazioni supplementari all'autorità di emissione. La consultazione può avvenire con qualsiasi mezzo appropriato ed è volta ad ottenere chiarimenti e documenti che completino il quadro conoscitivo, utile ad una decisione finale.

Nel solco di un procedimento che vuole garantire con consapevolezza il diritto ad essere informati, tutte le decisioni assunte sono comunicate immediatamente sia all'autorità di emissione sia al destinatario con ogni mezzo che consenta di conservare una traccia scritta.

Se l'autorità di emissione rigetta l'opposizione, il destinatario è obbligato a produrre i dati all'autorità di esecuzione e l'esecuzione avviene in conformità al diritto dello Stato di esecuzione¹²⁵³. L'inottemperanza è sanzionata con una sanzione pecuniaria¹²⁵⁴

¹²⁵¹ Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1352.

¹²⁵² In argomento, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 22.

¹²⁵³ Cfr., considerando n. 44, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹²⁵⁴ In argomento, S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, cit., p. 175.

effettiva, proporzionata e dissuasiva¹²⁵⁵, anche alla luce di circostanze specifiche come l'inottemperanza reiterata o sistematica¹²⁵⁶.

Ottenuti i dati elettronici, l'autorità di esecuzione li trasmette all'autorità di emissione entro due giorni lavorativi, a meno che tali dati siano protetti con un'immunità o un privilegio o siano soggetti alle norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione ai sensi del proprio diritto nazionale o incidano su interessi fondamentali del proprio Stato, come la sicurezza e la difesa nazionali. In tali casi informa l'autorità di emissione dei motivi della mancata trasmissione dei dati.

Orbene, almeno un difetto di coordinamento tra norme appare lampante. L'art. 14, par. 7 della proposta di Regolamento, sia in sede di riconoscimento che in sede di opposizione, consente all'autorità di esecuzione di consultare l'autorità di emissione con qualsiasi mezzo appropriato e, se del caso, chiedere ulteriori informazioni. Tuttavia, individua per la risposta un termine – invero, che appare ordinatorio – in capo all'autorità di emissione di cinque giorni lavorativi.

Ebbene, se il procedimento per il riconoscimento debba concludersi entro cinque giorni lavorativi, vi sarebbe una sovrapposizione dei termini, sicché, qualora sia

¹²⁵⁵ Le sanzioni sono irrogate conformemente al diritto dello Stato di esecuzione e contro esse ogni Stato membro deve assicurare un ricorso giurisdizionale effettivo. In merito alle sanzioni, si è affermato che «il rimettere la sanzione pecuniaria alla disciplina dello Stato membro di esecuzione dimostra l'atteggiamento "direttivo" che il Regolamento assume in taluni punti e potrebbe creare disparità di trattamento e operazioni di *forum shopping*. Invero, se un *provider* non fosse intenzionato a collaborare con le autorità per difendere la riservatezza dei dati dei propri clienti, o se volesse scongiurare il rischio di sanzioni pecuniarie elevate in caso di inottemperanza "colposa", allora ben potrebbe scegliere di stabilirsi (o trasferire la propria sede se già stabilito) nello Stato membro in cui le sanzioni pecuniarie sono le più miti. A ciò si aggiunga che vi può essere il rischio che gli Stati possano manovrare "al ribasso" le proprie scelte in merito alle sanzioni da irrogare (che comunque dovrebbero rimanere effettive, proporzionate e dissuasive), al fine di essere più competitivi e attrarre un maggior numero di SP sul proprio territorio. Pertanto sarebbe opportuno prevedere un meccanismo che elimini alla radice, o comunque attenui quanto più possibile, il rischio di *forum shopping*». Cfr., O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 24.

Sul punto va anche considerato che, nel disporre sanzioni in caso di violazione degli obblighi previsti agli artt. 9, 10 e 11, par. 1 della proposta di Regolamento, il legislatore europeo ha ritenuto opportuno stabilire delle sanzioni penali effettive, proporzionate e dissuasive, obbligando gli Stati a garantire che le sanzioni pecuniarie possano essere pari fino al 2% del fatturato mondiale totale annuo del prestatore di servizi nell'esercizio pendente. La disposizione, qualora sia estesa anche all'inosservanza degli obblighi di cui all'art. 14 della proposta di Regolamento, potrebbe aiutare ad armonizzare il sistema sanzionatorio europeo e favorire il superamento delle problematiche evidenziate.

Inoltre, ai sensi del *considerando* n. 45-*bis* della proposta di Regolamento, nel determinare nel caso di specie le opportune sanzioni pecuniarie, le autorità competenti dovrebbero tenere conto di tutte le circostanze pertinenti, quali la natura, la gravità e la durata della violazione, se è stata commessa intenzionalmente o per negligenza, se il fornitore del servizio è stato ritenuto responsabile per analoghe violazioni precedenti e la solidità finanziaria del prestatore di servizi ritenuto responsabile. In circostanze eccezionali, tale valutazione può portare l'autorità di esecuzione a decidere di astenersi dall'imporre sanzioni pecuniarie. A tale riguardo, particolare attenzione dovrebbe essere rivolta alle microimprese che non rispettano un ordine in caso di emergenza a causa della mancanza di risorse umane al di fuori del normale orario di lavoro, se i dati sono trasmessi senza indebiti ritardi.

Il sistema sanzionatorio così articolato ricorderebbe quello previsto per le sanzioni pecuniarie nell'ordinamento tedesco, basato sulla determinazione dei tassi ponderati in base alla situazione economica del sanzionato.

¹²⁵⁶ Cfr., *considerando* n. 45, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

consultata l'autorità di emissione, quasi certamente il riconoscimento non potrà avvenire nei termini individuati.

Bisognerebbe, dunque, armonizzare le disposizioni. La soluzione dovrebbe prevedere un allungamento dei termini per il riconoscimento, che siano comunque ragionevolmente funzionali ad evitare ritardi nel corso della procedura. È necessario individuare un bilanciamento tra le esigenze di una celere produzione dei dati elettronici volatili e la necessità di ottenere maggiori informazioni dall'autorità di emissione, per garantire una corretta valutazione, basata su un ampio ventaglio di elementi utili alla decisione finale.

9. Il principio del “diritto a difendersi, ricorrendo effettivamente”

Il legislatore europeo ha ritenuto che per uno strumento invasivo come l'ordine europeo di produzione sia necessario garantire il diritto ad un ricorso effettivo¹²⁵⁷.

Analogo mezzo di ricorso non è stato previsto per l'ordine europeo di conservazione. La scelta è stata giustificata dal fatto che la minore invasività dell'OEC e la finalità di conservazione – che non permette la divulgazione dei dati elettronici – consente di non ritenere necessario un ricorso. Tuttavia, qualora all'OEC segua un OEP o un altro strumento che comporta la divulgazione dei dati, il ricorso è possibile in virtù di questi strumenti¹²⁵⁸.

Si tratta, in effetti, di individuare uno strumento di garanzia volto a tutelare i diritti fondamentali che in qualche modo risultano limitati, lesi, intaccati dall'invasività dell'ordine europeo di produzione.

Se, dunque, è questa la finalità, in linea con quanto affermato dalla dottrina, sarebbe necessario prevedere un mezzo di ricorso anche per l'OEC, in un'ottica di bilanciamento tra le esigenze repressive e la tutela dei diritti fondamentali dei singoli¹²⁵⁹. Inoltre,

¹²⁵⁷ Sul punto, O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, cit., p. 27 ss.; R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, cit., p. 1355; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 288 ss.; V. TONDI, *L'accesso transfrontaliero all'elettronic evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 450 ss.

¹²⁵⁸ Cfr., *Relazione alla Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, p. 24.

¹²⁵⁹ In tal senso, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 292 ss., secondo i quali «va notato che la Commissione ha prestato la maggior parte delle sue attenzioni nei confronti dell'OPE (specie se concernente dati relativi alle operazioni o al contenuto), mentre ha tralasciato gli ordini di conservazione europei. Così facendo, ha dato vita per questi ultimi a un regime assai sbilanciato in favore delle esigenze repressive rispetto a quelle di tutela dei diritti fondamentali. Del resto, se è pur vero che la consegna dei dati informatici a un'autorità a fini penalistici incide in modo più gravoso sui diritti di un individuo rispetto al mero obbligo di conservarli inalterati, il fatto stesso che un individuo, per un certo periodo di tempo, non possa avere la libera disponibilità di informazioni che lo riguardano è comunque una forma di intrusione nella sua sfera di libertà, che pare necessitare di tutele più intense rispetto a quelle stabilite nella proposta in commento. A tale riguardo, basti pensare al fatto che, come accennato, la Commissione non ha neppure previsto che i destinatari di un OCE abbiano diritto a un *effective remedy* per contestare l'illegalità della misura. Questa scelta di politica normativa non pare affatto condivisibile, posto che sembra porsi in contrasto con l'art. 47, par. 1, della CDFUE. Tale disposizione della Carta di Nizza assicura, infatti, a ogni individuo che veda lesi i suoi diritti attribuiti dall'Unione – e quindi di certo anche a coloro nei cui confronti sia stato emanato un OCE – il diritto a un mezzo di ricorso effettivo. È di

l'assenza di un mezzo di ricorso potrebbe comportare la lesione proprio dell'art. 47, par. 1, della Carta dei diritti fondamentali dell'Unione europea.

L'art. 17, della proposta di Regolamento, prevede espressamente un diritto a un ricorso effettivo per le persone i cui dati sono richiesti, al fine di garantire i diritti e le libertà della persona che risultano violati. Il ricorso ha la finalità di verificare se l'ordine di produzione ha limitato illecitamente i diritti e le libertà della persona. La previsione, dunque, ricalca quanto indicato dall'art. 47, par. 1, della Carta dei diritti fondamentali dell'Unione europea¹²⁶⁰.

Il diritto ad un ricorso effettivo previsto all'art. 17, della proposta di Regolamento, è un autonomo rimedio¹²⁶¹ e va ad aggiungersi e non sostituirsi agli altri mezzi di ricorso disponibili nello Stato di emissione¹²⁶². Tale assunto appare confermato dall'incipit

conseguenza auspicabile che, nell'incedere dei lavori preparatori, le istituzioni UE ritornino sui loro passi e garantiscano espressamente la possibilità di esperire un "effective remedy" anche per gli ordini di conservazione europei». Sul punto, anche, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1288; V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 450 ss.

¹²⁶⁰ Sull'art. 47, della Carta dei diritti fondamentali dell'Unione europea, v., in dottrina, A. ARNULL, *The Principle of Effective Protection in EU Law: An Unruly Horse?*, in *European Law Review*, 1, 2011, p. 51 ss.; M. BORRACCETTI, *Art. 47*, in AA.VV., *La Carta dei diritti dell'Unione europea. Casi e materiali* (a cura di G. BISOGNI, G. BRONZINI, V. PICCONE), Taranto, 2009, p. 559 ss.; M. CONDINANZI, *Sub art. 47*, in AA.VV., *Commentario breve ai Trattati dell'Unione europea*, Padova, 2014, p. 1770 ss.; R. CONTI, *Il principio di effettività della tutela giurisdizionale ed il ruolo del giudice: l'interpretazione conforme*, in *Politica del diritto*, 3, 2007, p. 377 ss.; M. D'AMICO, *Articolo 47*, in AA.VV., *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea* (a cura di R. BIFULCO, M. CARTABIA, A. CELOTTO), Bologna, 2001, p. 319 ss.; G. D'AVINO, *Il diritto alla tutela giurisdizionale effettiva nell'art. 47 par. 1 della Carta dei diritti fondamentali dell'UE*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale del Titolo VI della Carta* (a cura di A. DI STASI), Napoli, 2019, p. 151 ss.; A. DI STASI, *Rispetto dei diritti fondamentali e spazio europeo di giustizia: a proposito del Titolo VI della Carta dei diritti fondamentali*, in AA.VV., *I diritti umani nella giurisprudenza e nella prassi del diritto internazionale ed europeo* (a cura di L. PANELLA), Torino, 2013, p. 327 ss.; D.P. DOMENICUCCI, F. FILPO, *La tutela giurisdizionale effettiva nel diritto dell'Unione europea*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea* (a cura di R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI), Milano, 2017, p. 864 ss.; L. FROMONT, A. VAN WAEBENBERGE, *La protection jurisdictionnelle effective en Europe ou l'histoire d'une procession d'Echternac*, in *Chaiers de droit européenne*, 1, 2015, p. 115 ss.; H. HOFFMAN, *Sub art. 47. Right to an Effective Remedy. Specific Provisions (Meaning)*, in AA.VV., *The EU Charter of Fundamental Rights. A Commentary* (a cura di S. PEERS, T. HERVEY, J. KENNER, A. WARD eds.), Oxford, 2014, p. 1211 ss.; F. KRENEC, *Article 47. Droit à un recours effectif et à accéder à un tribunal impartial*, in AA.VV., *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article* (F. PICOD, S. VAN DROOGHENBROECK eds.), Bruxelles, 2018, p. 981 ss.; A. LANG, *Il diritto ad un ricorso effettivo nell'Unione europea*, in AA.VV., *La tutela multilivello dei diritti* (a cura di P. BILANCIA, E. DE MARCO), Milano, 2004, p. 57 ss.; G. LEBRUN, *De l'utilité de l'article 47 de la Charte des droits fondamentaux de l'Union européenne*, in *Revue trimestrelle des droits de l'homme*, 106, 2016, p. 433 ss.; K. LENAERTS, *Le traité de Lisbonne et la protection jurisdictionnelle des particuliers en droit de l'Union*, in *Cahiers de droit européen*, 5-6, 2009, p. 711 ss.; I. PERNICE, *The Right to Effective Judicial Protection ad Remedies in the EU*, in AA.VV., *The Court of Justice and the Construction of Europe: analyses and Perspectives on Sixty Years of Case law* (A. ROSAS, E. LEVITS, Y. BOT eds.), Berlin, 2013, p. 381 ss.; M.J. RANGEL DE MESQUITA, *Sub art. 47*, in AA.VV., *Carta dos direitos fundamentais da União Europeia* (A. SILVEIRA, M. CANOTILHO eds.), Coimbra, Almedina, 2013, p. 537 ss.

¹²⁶¹ In tal senso, A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., 272.

¹²⁶² Inoltre, non pregiudica la possibilità di usufruire dei mezzi di ricorso previsti dalla direttiva 2016/680/UE sulla protezione dei dati nelle attività di polizia e giustizia e del Regolamento UE 2016/679 sulla protezione dei dati. Sul punto, R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in*

dell'articolo secondo cui sono «fatti salvi ulteriori mezzi di ricorso disponibili ai sensi del diritto nazionale».

Nello specifico, il ricorso è esercitato nello Stato di emissione da qualsiasi persona i cui dati sono stati ricercati, pur non essendo indagati o imputati in un procedimento penale. Ove indagata o imputata, tale persona ha diritto a un ricorso effettivo durante il procedimento penale in cui i dati vengono utilizzati, e che può incidere sull'ammissibilità di questi.

Il diritto va esercitato innanzi un organo giurisdizionale dello Stato di emissione in conformità al diritto nazionale di tale Stato e include la possibilità di contestare la legittimità della misura, comprese la sua necessità e la sua proporzionalità. Il termine "include" farebbe intendere che il mezzo di ricorso possa essere esperito anche per il merito. Invero, il Regolamento non sembra limitare i possibili motivi adducibili per contestare un ordine europeo di produzione.

Ovviamente, la formulazione non indica per ogni singolo Stato membro quale sia l'organo giurisdizionale competente, nel rispetto del principio di non ingerenza. Si sarebbe, quindi, al cospetto di una norma aperta, che necessita di un intervento di adattamento negli ordinamenti nazionali.

Pertanto, è ipotizzabile, anche in tal caso, che al Regolamento succederanno uno o più atti di esecuzione da parte degli Stati membri, in virtù di una disciplina non pienamente *self-executing* e che manifesta la necessità di determinare alcuni elementi fondamentali per la pratica attuazione.

Orbene, la norma individua tra i legittimati non solo gli indagati e gli imputati, ma anche qualsiasi persona i cui dati sono stati ricercati. *Prima facie*, la platea dei legittimati sembra particolarmente ampia. Tuttavia, sembrerebbe opportuno estendere la legittimazione anche ad altri portatori di interessi.

Infatti, nell'ambito di un procedimento per ordine europeo di produzione, il dato sequestrato potrebbe contenere un bagaglio di informazioni relative non solo alla persona i cui dati siano stati ricercati, ma anche a persone i cui dati non sono stati ricercati. In questo caso, la persona interessata sembra non avere alcun diritto ad un ricorso effettivo, con conseguente lesione dei diritti garantiti dalla Carta dei diritti fondamentali dell'Unione europea.

Tenuto conto che ai sensi dell'art. 3, par. 2, della proposta di Regolamento, «gli ordini possono essere emessi anche per procedimenti relativi a reati per i quali una persona giuridica può essere considerata responsabile o punibile nello Stato di emissione», sarebbe opportuno prevedere la legittimazione anche in capo alle persone giuridiche portatrici di un interesse, i cui dati non siano stati ricercati¹²⁶³, nei cui confronti vi sia una asserita lesione dei diritti causata da un'apprensione involontaria di dati sensibili e/o segreti.

È necessario, inoltre, che alle persone legittimate al ricorso siano assicurate le garanzie procedurali, tra cui il diritto all'informazione. Ed invero, l'art. 17, par. 4, della proposta di Regolamento attribuisce all'autorità di emissione l'onere di adottare tutte le misure

UE: la proposta di Regolamento e-evidence, cit., p. 1355; V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 451.

¹²⁶³ Si pensi all'ipotesi in cui, nell'ambito di una ricerca di dati relativi ad una persona, si ricavano anche dati ultronei, relativi ad informazioni particolarmente sensibili ovvero a segreti industriali. In tal caso, la norma non chiarisce, ma anzi, sembra escludere la possibilità di un ricorso effettivo che si muova nella direzione della tutela della riservatezza, a fronte di una chiara violazione di un diritto fondamentale.

necessarie a garantire che siano fornite informazioni sulla possibilità di ricorso ai sensi del diritto nazionale e per garantire l'esercizio effettivo.

Anche qui, i legislatori nazionali dovranno individuare il momento in cui inviare l'informazione a garanzia del diritto di difesa. Verosimilmente, dovrebbe essere individuato nel primo atto con cui la persona interessata viene a conoscenza di un procedimento per ordine europeo di produzione.

Sul punto, invero, si esprime anche la proposta di Regolamento all'art. 11¹²⁶⁴, con il quale si contemperano le esigenze di segretezza delle indagini con la tutela della riservatezza dei diritti delle persone coinvolte e il diritto ad essere informati, per l'esercizio del diritto di difesa¹²⁶⁵.

Nello specifico, con la trasmissione dell'EPOC o dell'EPOC-PR, l'autorità di emissione ha tre alternative: chiedere al destinatario o al prestatore di servizi di informare la persona i cui dati sono ricercati; informare essa stessa la persona i cui dati sono ricercati in conformità alle misure nazionali di attuazione di cui all'art. 13 della direttiva 2016/680/UE sulla protezione dei dati nelle attività di polizia e giustizia¹²⁶⁶; ovvero posticipare l'informazione della persona i cui dati sono ricercati per tutto il tempo in cui ciò costituisca una misura necessaria e proporzionata¹²⁶⁷ per non ostacolare il procedimento penale¹²⁶⁸. Nei primi due casi, il diritto ad essere informati è garantito includendo anche tutte le informazioni necessarie sui mezzi di ricorso disponibili a norma dell'art. 17 della proposta di Regolamento.

Dunque, l'informazione appare essenziale per consentire il controllo giurisdizionale e il ricorso in sede giudiziale. Sarebbe, quindi, espressione dell'esercizio del diritto di difesa e attività prodromica e funzionale all'instaurazione di un successivo contraddittorio.

Non mancano nell'art. 17, della proposta di Regolamento, indirizzi volti ad ottenere discipline organiche e sistematiche. Invero, il par. 5 richiede che i termini o le altre condizioni per la proposizione del ricorso siano uguali a quelli previsti in casi interni

¹²⁶⁴ La disposizione si ispira all'art. 19 della direttiva 2014/41/UE in materia di ordine europeo di indagine.

¹²⁶⁵ In tal senso, M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, cit., p. 1287; M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 287; V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 450. In particolare, l'art. 11 della proposta di Regolamento prevede un obbligo di riservatezza dell'EPOC o dell'EPOC-PR e dei dati prodotti o conservati gravante sul destinatario e sul prestatore di servizi. Inoltre, non sono tenuti ad informare la persona i cui dati sono riservati, salvo richiesta contraria formulata dall'autorità di emissione.

¹²⁶⁶ La direttiva è stata recepita con d.lgs. 18 maggio 2018, n. 51, in GU n. 119 del 24 maggio 2018. L'art. 13 della direttiva 2016/680/UE è relativo alle informazioni da rendere disponibili o da fornire all'interessato ed in Italia è stato recepito all'art. 10 del d.lgs. 18 maggio 2018, n. 51.

¹²⁶⁷ Parte della dottrina ritiene che la disposizione in esame sacrifichi eccessivamente i diritti della persona i cui dati sono ricercati. Invero, la posticipazione dell'informazione per un tempo necessario e proporzionato appare una limitazione delle prerogative difensive che non può essere rimessa alla sola valutazione dell'autorità di emissione, ma richiede un vaglio da parte di un'autorità giurisdizionale che compensi la compressione dei diritti riconosciuti dall'ordinamento. Sul punto, O. POLLICINO, M. BASSINI, *La proposta di regolamento e-Evidence: osservazioni a caldo e possibili sviluppi*, cit., p. 1 ss.

¹²⁶⁸ Volendo precisare, la ricerca di un bilanciamento tra tutti gli interessi delle parti in gioco e degli interessi pubblicistici emergenti ha comportato l'inserimento all'art. 11, par. 3, della proposta di Regolamento, di un'inedita disposizione – invero, sin troppo discrezionale – che apre la strada ad una quarta decisione possibile sul tema da parte dell'autorità di emissione, la quale può astenersi dall'informare la persona di cui sono ricercati i dati relativi agli abbonati ed agli accessi ove necessario e proporzionato per tutelare i diritti fondamentali e legittimi di un'altra persona, in particolare nel caso in cui tali diritti e interessi prevalgano sull'interesse di essere informata della persona i cui dati sono ricercati.

analoghi e siano applicati in modo da garantire alle persone interessate l'esercizio effettivo del ricorso.

Evidenti gli obiettivi che si vogliono raggiungere con un ricorso effettivo: garantire il diritto di difesa ed il giusto processo¹²⁶⁹. In particolare, il sistema di ricorso immaginato dall'Unione europea è volto a garantire quello che potrebbe definirsi il “diritto di difendersi, ricorrendo effettivamente”, laddove il mezzo di ricorso non deve solo in astratto garantire il principio di legalità e i diritti fondamentali, ma in concreto dimostrare di essere efficace ed effettivo per eliminare ogni abuso, illiceità o illegittimità nell'uso di uno strumento particolarmente invasivo come l'ordine europeo di produzione.

Orbene, la scelta di prevedere un diritto ad un rimedio effettivo per l'ordine europeo di produzione è innovativa perché sembra richiedere l'elaborazione di un autonomo mezzo di impugnazione¹²⁷⁰.

I principi e gli obiettivi fissati devono tradursi in norme chiare ed applicabili, sicché sembra necessario comprendere cosa si intende per “ricorso effettivo”: il diritto ad un ricorso effettivo richiederebbe un rimedio giurisdizionale idoneo allo scopo, in mancanza del quale risulterebbe violato il diritto alla tutela giurisdizionale effettiva.

Il legislatore nazionale sarebbe chiamato a creare un rimedio che sia sostanzialmente efficace, ispirandosi ai principi di equivalenza ed effettività. In termini diversi, il ricorso dovrebbe garantire in concreto ai singoli la tutela dei diritti coinvolti con il procedimento dell'ordine europeo di produzione. Inoltre, il ricorso non deve essere meno favorevole rispetto ai ricorsi analoghi di natura meramente interna¹²⁷¹.

Invero, un ricorso non risulta essere effettivo qualora renda praticamente impossibile o eccessivamente difficile l'esercizio dei diritti conferiti ai singoli dal diritto dell'Unione. È necessario che siano in concreto tutelati i diritti della difesa, il principio della certezza del diritto ed il regolare svolgimento del procedimento¹²⁷². Una simile condizione si realizza anche quando uno Stato membro non renda eccessivamente difficile o praticamente impossibile il ricorso.

È necessario, dunque, che il ricorso preveda l'esame completo ed *ex nunc* degli elementi di fatto e di diritto, analizzando l'effettivo rispetto delle norme e dei principi alla base del Regolamento e degli atti legislativi che ne deriveranno nell'ordinamento interno.

Di conseguenza, anche il provvedimento finale deve effettivamente spiegare effetti a tutela di chi ha proposto ricorso ed ha visto riconoscersi i diritti. Invero, qualora il ricorso sia accolto, il materiale dovrebbe essere dichiarato inutilizzabile.

Del resto, anche per l'ordine europeo di produzione non può che valere quanto già statuito per l'ordine europeo di indagine dalla Corte di giustizia, secondo cui la garanzia dei diritti spetta in primo luogo allo Stato membro di emissione, che si deve presumere rispetti il diritto dell'Unione e, in particolare, i diritti fondamentali riconosciuti da quest'ultimo¹²⁷³.

¹²⁶⁹ Cfr., art. 17, par. 6 della proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

¹²⁷⁰ Per un approfondimento sull'*effective remedy* previsto per l'ordine europeo di produzione, v. A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., 270 ss.

¹²⁷¹ Sul punto, si rinvia a Corte di giustizia, Grande Sezione, sentenza 13 marzo 2007, causa C-432/05, *Unibet (London) Ltd e Unibet (International) Ltd*, punto 43.

¹²⁷² Cfr., Corte di giustizia, sentenza del 27 giugno 2013, causa C-93/12, *ET Agroconsulting-04-Velko Stoyanov*, punto 48.

¹²⁷³ In tal senso, Corte di giustizia, sentenza del 23 gennaio 2018, causa C-367/16, *Piotrowski*, punto 50.

Come acutamente già osservato per l'ordine europeo d'indagine¹²⁷⁴, secondo cui l'art. 14 della direttiva 2014/41/UE opera una netta distinzione tra impugnazioni dell'atto di indagine e impugnazione dell'ordine europeo d'indagine con il quale si richiede l'atto stesso, anche per l'ordine europeo di produzione bisognerebbe mantenere questa distinzione, dovendo creare con il ricorso effettivo di cui all'art. 17 della proposta di Regolamento un mezzo di impugnazione finalizzato a verificare la legalità del provvedimento.

Orbene, siccome l'OEP si affianca all'OEI ed entrambe sono procedure *in rem*, è opportuno che le discipline relative ai ricorsi si coordinino sistematicamente. Purtroppo, già dall'attuale disciplina in esame sembrano ravvisarsi zone d'ombra.

L'impugnazione non segue l'atto d'indagine ma lo strumento utilizzato, sicché sarà possibile individuare il corrispondente mezzo di ricorso, in ragione dello strumento di cooperazione attivato. Tale sistema potrebbe portare l'autorità di emissione a compiere scelte strategiche in relazione al possibile mezzo di ricorso esperibile da parte della persona i cui dati sono ricercati, con evidenti ripercussioni sugli effetti e sulle scelte che dovrà compiere la difesa.

Ciò è particolarmente evidente se si pensa che attualmente nell'ordinamento italiano l'unico mezzo di impugnazione possibile a fronte di una procedura attiva mediante OEI è previsto all'art. 28 d.lgs. 21 giugno 2017, n. 108 per i sequestri probatori, laddove per gli altri atti d'indagine si ravviserebbe un vuoto normativo, tanto evidente se si considera quanto di recente affermato dalla Corte di giustizia dell'Unione europea¹²⁷⁵.

Orbene, in relazione alle scelte che dovrà compiere il legislatore italiano, pare che il legislatore possa percorrere più strade per garantire un ricorso effettivo: prevedere un mezzo di ricorso del tutto nuovo; scegliere un modello basato su quanto previsto dal combinato disposto degli artt. 257 e 324 c.p.p.¹²⁷⁶; optare per una opposizione simile a quella prevista all'art. 13, comma 7, d.lgs. 21 giugno 2017, n. 108. Già in passato si è detto che quest'ultima alternativa sembra la più opportuna, perché garantisce la

¹²⁷⁴ Sul punto, D. CIMADOMO, *Ordine europeo di indagine penale e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, cit., p. 230, il quale adombrava la possibilità di un possibile mezzo di ricorso nello Stato di emissione relativo all'ordine europeo di indagine diverso da quello relativo all'atto di indagine. Di recente, anche la giurisprudenza europea sembra andare in tale direzione. Invero, si è detto che non è compatibile con il diritto dell'Unione una normativa nazionale che non preveda rimedi avverso la emissione di un OIE finalizzato allo svolgimento di perquisizioni e di sequestri ed all'organizzazione di un'audizione di testimoni mediante videoconferenza. Sebbene la sentenza si concentri su questi due specifici atti d'indagine, il principio sembra estensibile anche agli altri atti. Invero, se per il sequestro probatorio sembra applicabile e sufficiente quanto stabilito dall'art. 28, d.lgs. 21 giugno 2017, n. 108, non sembrano previsti rimedi rispetto all'OEI emesso negli altri casi. Cfr., Corte di giustizia, sentenza 11 novembre 2021, causa C-852/19, *Ivan Gavanozov*, punto 62.

¹²⁷⁵ Cfr., Corte di giustizia, sentenza 11 novembre 2021, causa C-852/19, *Ivan Gavanozov*, punto 56, secondo cui «l'impossibilità di contestare nello Stato membro di emissione la necessità e la regolarità di un ordine europeo di indagine avente ad oggetto lo svolgimento di perquisizioni e di sequestri nonché l'organizzazione di un'audizione di testimoni mediante videoconferenza, quanto meno alla luce delle ragioni di merito della sua emissione, costituisce una violazione del diritto a un ricorso effettivo sancito all'articolo 47 della Carta, con la conseguenza che il riconoscimento reciproco non può trovare applicazione e andare a beneficio di tale Stato membro».

¹²⁷⁶ Su tale posizione, V. TONDI, *L'accesso transfrontaliero all'elettronica evidence, tra esigenze di effettività e tutela dei diritti*, cit., p. 451, secondo cui si potrebbe ipotizzare un mezzo di ricorso analogo alle previsioni in materia di impugnazione del provvedimento di sequestro probatorio di dati relativi a sistemi informatici o telematici, ex artt. 254-bis e 257 c.p.p., nell'ambito del procedimento penale aperto nello Stato di emissione.

sistematicità delle impugnazioni degli ordini. In questo modo, si eviterebbe di creare possibili aporie o riduzioni di garanzie del diritto di difesa¹²⁷⁷.

L'affermazione merita un chiarimento. Sarebbe opportuno che il nuovo ricorso effettivo sia proiettato a controllare il provvedimento con cui è stato emesso l'ordine di produzione in punto di legittimità e di merito, staccandosi dalle valutazioni relative all'atto di indagine compiuto, per il quale sarebbe possibile esperire l'idoneo mezzo di impugnazione già previsto dall'ordinamento interno.

Dunque, il ricorso dovrebbe assumere una conformazione simile a quella prevista dall'art. 13, comma 7, d.lgs. n. 108/2017, ma, a differenza di quest'ultimo, dovrebbe essere azionato nello Stato di emissione nei confronti del provvedimento con cui si emette l'ordine e non, come accade con l'OEI, nei confronti del decreto di riconoscimento, giacché per la particolarità dell'ordine europeo di produzione un decreto di riconoscimento non è generalmente previsto.

Oltre a contestare l'ordine di produzione in punto di necessità e proporzionalità, il "diritto di difendersi, ricorrendo effettivamente" dovrebbe lasciare alla persona i cui dati sono ricercati la possibilità di contestare un ordine che asseritamente non è stato emesso o convalidato da un'autorità non legittimata ai sensi dell'art. 4, della proposta di Regolamento, o non è stato emesso per un reato non compreso nell'elenco dei reati-presupposto di cui all'art. 5, par. 4 della proposta di Regolamento e per cui non è possibile richiedere un ordine. Si potrebbe anche pensare a un ricorso nei confronti di un ordine di produzione emesso nell'ambito di un servizio non riconducibile al Regolamento ovvero in presenza di un privilegio, di una immunità, di norme sulla determinazione e limitazione della responsabilità penale relative alla libertà di stampa e alla libertà di espressione in altri mezzi di comunicazione.

L'innovatività del ricorso effettivo si apprezza anche per le ricadute che un simile istituto può avere nel processo. In particolare, l'art. 17, par. 6, della proposta di Regolamento, richiede che nei procedimenti penali nello Stato di emissione siano rispettati i diritti della difesa e sia garantito un giusto processo nel valutare le prove acquisite tramite l'ordine europeo di produzione¹²⁷⁸.

La disposizione aprirebbe ad una inedita forma di inammissibilità delle prove, sanzione che non ha mai avuto grande seguito nelle fonti dell'Unione europea in materia di cooperazione giudiziaria in materia penale.

In particolare, si prevederebbe espressamente che la violazione delle norme europee incida sulla legale formazione della prova, sino al punto da decretarne l'inammissibilità ovvero, a seconda dei casi, incidere sul peso di tali prove nell'ambito del procedimento¹²⁷⁹.

Il mancato rispetto dei diritti di difesa e del giusto processo, nonché del principio di legalità e dei diritti fondamentali, può comportare, quale conseguenza, l'inammissibilità degli elementi di prova elettronici raccolti con lo strumento dell'ordine europeo di produzione nel relativo procedimento penale per cui sono state richieste.

¹²⁷⁷ Sia consentito il rinvio ad A. GAUDIERI, *Opposizione al decreto di riconoscimento dell'ordine europeo di sequestro: scenari*, cit., p. 2034 ss.

¹²⁷⁸ In tal senso, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 288

¹²⁷⁹ Cfr., considerando n. 54, Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

In ciò è ravvisabile un profilo di divergenza con la disciplina prevista dalla direttiva 2014/41/UE¹²⁸⁰, laddove si limita all'art. 14, par. 7, ad indicare allo Stato di emissione di tener conto «del fatto che il riconoscimento o l'esecuzione di un OEI sono stati impugnati con successo conformemente al proprio diritto nazionale», senza però accennare ad eventuali conseguenze¹²⁸¹.

Orbene, va comunque chiarito che per l'ordinamento italiano più che di inammissibilità – causa di invalidità che impedisce al giudice di esaminare nel merito una richiesta avanzata da una parte del procedimento, quando la richiesta non ha i requisiti richiesti dalla legge – si dovrebbe parlare, in applicazione dell'art. 191, comma 1, c.p.p., di inutilizzabilità, essendo questa un tipo di invalidità che colpisce il valore probatorio dell'atto¹²⁸².

In sostanza, non si può che apprezzare la scelta compiuta dal legislatore europeo di assumere una posizione radicale e decisa a favore delle garanzie processuali ed in particolare del diritto di difesa.

In particolare, nell'indicare quale criterio di valutazione il rispetto dei diritti di difesa e del giusto processo, il legislatore europeo non ha voluto concentrare la propria attenzione solo sui quattro pilastri (contraddittorio, sostanziale parità delle parti, giudice terzo ed imparziale nonché ragionevole durata del procedimento), ma anche su tutto il fascio di diritti del processo e nel processo che emergono indubbiamente da una lettura sistematica dell'art. 6 CEDU e dell'art. 47 della Carta dei diritti fondamentali dell'Unione europea¹²⁸³.

¹²⁸⁰ Cfr., A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., p. 261, secondo cui pur prescrivendo delle regole procedurali, l'ordine europeo di indagine resta silente «in merito ad eventuali conseguenze derivanti dalla loro violazione». V., anche, F. SIRACUSANO, *The European Investigation Order for Evidence Gathering Abroad*, cit., p. 97, secondo cui «no mention is made in the European Directive to a regime which excludes gathered evidence; in line with the European legislator to pay no particular attention to procedural invalidity».

¹²⁸¹ Sul punto, A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., p. 273 e 262, secondo cui «nessun obbligo viene dunque esplicitamente previsto, in capo allo Stato di esecuzione, di trattenere le prove raccolte, oppure, per quello di emissione, che già ne sia venuto in possesso, di impedirne l'uso da parte dei propri giudici; la sospensione del trasferimento, in pendenza di impugnazione, è infatti una mera eventualità».

¹²⁸² In argomento, P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 206, secondo cui «il termine “inutilizzabilità” descrive due aspetti del medesimo fenomeno. Da un lato, esso indica il “vizio” da cui può essere affetto un atto (causa); da un altro lato, esso illustra il “regime giuridico” al quale l'atto viziato è sottoposto (effetto), e cioè il non poter essere messo a fondamento di una decisione del giudice oppure di un atto del pubblico ministero o della polizia giudiziaria.

L'inutilizzabilità è un tipo di invalidità che ha la caratteristica di colpire non l'atto in sé, bensì il suo “valore probatorio”. L'atto, pur valido dal punto di vista formale (ad esempio, non è affetto da nullità), è colpito nel suo aspetto sostanziale, poiché l'inutilizzabilità impedisce ad esso di produrre il suo effetto principale, che è quello di essere posto a base di una decisione».

Sull'inutilizzabilità, v., inoltre, A. MARANDOLA, *La patologia dell'atto processuale: indirizzi sostanziali vs legalità formale*, in *Dir. pen. e proc.*, 9, 2012, p. 1059, secondo cui il sistema attuale conduce verso possibili e deprecabili sovrapposizioni tra invalidità (nullità e inutilizzabilità; prova inutilizzabile e prova illecita; nullità e abnormità, abnormità e irregolarità), con il serio rischio di lesione del principio di legalità.

¹²⁸³ In dottrina, infatti, si è affermato, quasi abbracciando una visione giusnaturalistica, che il giusto processo rimanda a un concetto ideale di Giustizia, che preesiste alla legge e che è direttamente collegato ai diritti inviolabili di tutte le persone coinvolte in un processo, che un ordinamento si impegna a riconoscere. In tal senso, P. TONINI, C. CONTI, *Manuale di procedura penale*, cit., p. 39. In argomento, anche, A. DE CARO, voce *Giusto processo*, in *I dizionari sistematici, Procedura penale* (a cura di G. SPANGHER), Milano, 2008, p. 26, in cui l'A. ritiene che il termine “giusto processo” «ha sia un indiscutibile valore riepilogativo dei diritti, non solo costituzionali, ma anche convenzionali: se si isolasse dal contesto

Ma una lettura limitata a soli questi articoli appare fortemente riduttiva. La vera portata di questa forma di inammissibilità si potrebbe estendere sino a ricomprendere anche altri diritti fondamentali coinvolti. La valutazione della necessità e proporzionalità della misura adottata sembrerebbe consentire l'ingresso ad altri diritti coinvolti quali il rispetto della vita privata e familiare, la protezione dei dati di carattere personale, la libertà di pensiero, di coscienza e di religione, nonché di espressione. Insomma, una serie di diritti fondamentali già declinati o in futuro declinabili quali “nuovi diritti” alla luce del progresso tecnologico.

A differenza di quanto avviene per l'ordine europeo di indagine, i rilievi in punto di necessità e di proporzionalità consentirebbero alla persona i cui dati sono ricercati di far valere in sede di ricorso i propri diritti nei confronti di attività investigative tecnologicamente avanzate che incidono sulle libertà fondamentali, ottenendo, in caso di accoglimento del ricorso, una restrizione dell'uso probatorio degli elementi elettronici ottenuti, qualora si instauri il processo, e ristabilendo in concreto la sostanziale correttezza del giusto processo.

Dunque, nell'introdurre un “*effective remedy*”, l'intenzione del legislatore europeo sarebbe quello di consentire un vaglio sui parametri di legittimità propri non solo dell'ordinamento nazionale, ma anche delle fonti sovranazionali.

Di certo non si può nascondere che già altre disposizioni del diritto dell'Unione europea prevedevano sostanzialmente il rispetto dei diritti di difesa e del giusto processo¹²⁸⁴, come già è attestata la tecnica di riprodurre in atti di diritto derivato la disposizione di cui all'art. 47, par. 1, della Carta dei diritti fondamentali¹²⁸⁵. Tuttavia, l'elemento di assoluta novità sta nell'aver adottato una previsione più coraggiosa in tema di rimedi rispetto agli atti di diritto derivato del passato in materia di cooperazione giudiziaria penale¹²⁸⁶.

delle garanzie richiamate avrebbe, infatti, una difficile traduzione procedurale. Ciò nonostante, però, il richiamo costituzionale riveste anche un evidente valore aggiunto rispetto al contesto esistente. Ha, invero, anche un'indiscutibile vocazione sistematica perché disegna una relazione tra garanzie soggettive e oggettive riconducendole a sistema processuale»; P. FERRUA, *Il “giusto processo”*, Bologna, 2005, p. 32, secondo cui la formula “giusto processo” è di incerto significato giuridico in quanto i connotati del “giusto” processo sono definiti altrove. Secondo G. SPANGHER, *Il “giusto processo” penale*, in *Studium Iuris*, 2000, p. 256, si tratterebbe di un concetto limite, funzionale ad orientare nella scelta delle diverse soluzioni processualmente possibili. A giudizio di N. TROCKER, *Il valore costituzionale del “giusto processo”*, in AA.VV., *Il nuovo articolo 111 della Costituzione e il giusto processo civile* (a cura di M. G. CIVININI E C.M. VERARDI), Milano, 2001, p. 45, il termine indicherebbe gli stessi principi enunciati successivamente nelle varie fonti in cui è previsto, visti nel loro dinamico combinarsi in una dimensione concreta e fattuale.

¹²⁸⁴ Si pensi all'art. 12, par. 2 della direttiva 2013/48/UE relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari, ed all'art. 10, par. 2 della direttiva 2016/343/UE sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali.

¹²⁸⁵ Si pensi, ad esempio, alla direttiva 2013/48/UE, alla direttiva 2016/343/UE, alla direttiva 2016/800/UE sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali nonché la direttiva 2016/1919/UE sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo. Per una panoramica sui rimedi previsti dalle cc.dd. direttive di Stoccolma, A. CABIALE, *I limiti alla prova nella procedura penale europea*, cit., p. 207 ss.

¹²⁸⁶ In tal senso, M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, cit., p. 288 ss.

Le disposizioni analizzate testimoniano l'emergere di un procedimento penale europeo, con norme proprie, che deve sempre trovare un equilibrio tra la sicurezza dei cittadini e la tutela dei diritti fondamentali¹²⁸⁷.

Non si può, a tale punto, non constatare che grazie agli influssi provenienti dall'Unione europea, il processo penale va verso una maggior attenzione all'ambito sostanziale, fondandosi su parametri di giudizio basati su canoni di razionalità pratica, anziché di razionalità astratta¹²⁸⁸.

Non più solo rispetto del modello legale di formazione della prova, ma anche concreta attenzione al rispetto dei diritti fondamentali. Infatti, ben potrebbe esserci un rispetto formale del modello legale, ma, in concreto, la lesione di un diritto fondamentale che dovrà comportare l'inutilizzabilità del dato probatorio per quel determinato processo, al fine di garantire una corretta decisione finale.

¹²⁸⁷ Così, H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, cit., p. 433 ss.

¹²⁸⁸ In tal senso, R. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in *Riv. It. Dir. e proc. pen.*, cit., p. 1191 ss.

CAPITOLO V

RILIEVI CONCLUSIVI

Sommario: 1. Sfide future in tema di *e-evidence* transnazionale. – 2. Le comuni e nuove incertezze. – 3. Sull’abbandono del principio di territorialità. – 4. Il ruolo propulsivo dell’Unione europea: un’ambizione possibile. – 5. Secondo protocollo addizionale alla Convenzione sulla criminalità informatica e attività dell’Unione europea. – 6. La vera “sfida” dell’Unione europea: l’efficienza degli ordini europei di produzione e di conservazione. – 7. Ampliamento del diritto di difesa *versus* limitazione delle investigazioni difensive. – 8. Tecnologia e diritti fondamentali. A lezione dai classici per possibili azioni bilanciate.

1. Sfide future in tema di *e-evidence* transnazionale

L’impatto di internet sulla società è dirompente. Il mondo digitale ha una veste del tutto diversa da quella che usualmente si è abituati a vedere. Si tratta di un mondo senza confini, dove le informazioni sono accessibili, condivise e libere di fluire senza impedimenti.

Le nuove tecnologie hanno donato un nuovo senso di libertà ai popoli ed alle società. Internet è un potente propulsore per il progresso scientifico. Se il mondo è riuscito a combattere la pandemia è anche grazie alla digitalizzazione, che ha permesso la condivisione di dati ed informazioni in tempo reale utili – *inter alia* – dapprima per la conoscenza e poi per lo sviluppo di vaccini o terapie per la cura del covid-19.

Tuttavia, è in questo mondo, strettamente connesso a quello reale, che si annidano nuove forme di criminalità. Oggi, la maggior parte dei reati è si consuma in ambienti digitali o coinvolge elementi informatici, che se scoperti, possono rivelare informazioni importantissime sul fatto.

Internet deve restare uno spazio libero, ma non per questo deve assumere la forma di un territorio ove sono consentite anche condotte riprovevoli e lesive dei beni giuridicamente protetti. Infatti, il diritto è entrato nella società tecnologica, tanto da poter formulare in chiave moderna il brocardo “*ubi societas tecnologica, ibi ius*”¹²⁸⁹.

Come facilmente intuibile, la lotta alla criminalità informatica continua a rappresentare una delle sfide principali per la nostra società. Il mondo di internet è di fatto senza frontiere. Di conseguenza, le indagini sono quasi sempre transfrontaliere ed esigono una stretta cooperazione tra le autorità di Paesi terzi.

In questo contesto, l’acquisizione degli elementi informatici collocati all’estero ed aventi attitudine probatoria acquista un ruolo centrale per le indagini penali e, successivamente, per il processo, in quanto sovente unici elementi in grado di consentire la ricostruzione di un fatto-reato.

Le informazioni utili sono sempre più spesso detenute in forma elettronica dai prestatori di servizi in altri ordinamenti statuali. Una risposta efficace della giustizia penale richiede misure adeguate a ottenere tali prove al fine di rispettare lo stato di diritto.

¹²⁸⁹ Per tale espressione, T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Il diritto dell’informazione e dell’informatica*, 3, 2020, p. 465.

In ambito internazionale, europeo e nazionale si sta cercando di migliorare l'accesso transfrontaliero alle prove elettroniche per le indagini penali in tutto il mondo. Per fare ciò, nel settore internazionale è necessario creare norme compatibili per evitare sovrapposizioni normative.

Per uniformità, potrebbe rivelarsi opportuno concludere una nuova Convenzione sulla criminalità informatica all'interno delle Nazioni Unite. Tuttavia, nonostante gli sforzi profusi¹²⁹⁰, pare che i tempi non siano ancora maturi.

Pertanto, la Convenzione di Budapest rimane la principale convenzione multilaterale in materia di lotta contro la criminalità informatica e l'entrata in vigore del Secondo protocollo lo confermerà.

Intanto, a livello regionale si stanno facendo buoni progressi e bisogna in ogni caso incentivare lo scambio delle migliori pratiche, evitando che si duplichino le fonti.

La firma di un Secondo protocollo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione di prove elettroniche, la disciplina statunitense prevista con il CLOUD Act e gli ordini europei di produzione e conservazione sono da salutare con favore perché consentono di garantire lo stato di diritto, la certezza dei rapporti e delle leggi nonché, più in generale, il principio di legalità¹²⁹¹.

Senza queste fonti, l'acquisizione di dati elettronici continuerebbe ad avvenire con i classici strumenti rogatoriali, dimostratisi sin troppo lenti. L'inefficacia di questi è dimostrata dal fatto che, spesso, al momento dell'esecuzione, i dati elettronici risultano alterati, modificati, cancellati, con conseguente dispendio di energie, mezzi e forze. Attività di questo tipo spesso si rivelano del tutto inutili.

Innanzitutto a tale situazione, gli Stati hanno reagito sviluppando una prassi che, tuttavia, non mette al centro il principio di legalità. Invero, la cooperazione con i fornitori di servizi di frequente avviene su base volontaria. Sulla scorta di tale prassi, le autorità pubbliche chiedono la conservazione o la produzione di dati anche quando i fornitori di servizi non sono obbligati a farlo.

Sebbene ciò abbia riportato ottimi risultati, restano però ampie zone d'ombra, colmabili unicamente con una disciplina di settore specifica che consenta di garantire il principio di legalità, la certezza del diritto, lo stato di diritto, comprimendo l'ampia

¹²⁹⁰ Cfr., Risoluzione 74/247 dell'Assemblea generale delle Nazioni Unite, del dicembre 2019, sul contrasto all'uso di tecnologie dell'informazione e della comunicazione a scopi criminali. L'Assemblea ha deciso di istituire un comitato intergovernativo di esperti *ad hoc* a tempo indeterminato, in rappresentanza di tutte le regioni, per elaborare un Convenzione internazionale sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali. In tal modo, l'Assemblea terrà in piena considerazione gli strumenti globali esistenti e gli sforzi per combattere l'uso delle tecnologie dell'informazione e della comunicazione a fini criminali, compreso, in particolare, il lavoro del gruppo di esperti intergovernativo aperto per condurre uno studio completo sulla criminalità informatica.

¹²⁹¹ In merito al principio di legalità, si è detto che si tratta di una norma di riconoscimento del diritto positivo esistente. In tale accezione, il principio di legalità equivale al principio di positività e, pertanto, è diritto tutto e solo quello che è posto dall'esercizio di poteri conferiti dal diritto nelle forme, quali che siano, dal diritto medesimo stabilite. In tal senso, L. FERRAJOLI, *La costruzione della democrazia. Teoria del garantismo costituzionale*, Bari-Roma, 2021, p. 75. Così definito, il principio corrisponderebbe all'uso tedesco di *Rechtsstaat*, e sarebbe alla base di tutti gli ordinamenti giuridici moderni nei quali i pubblici poteri hanno una fonte legale dalla quale soltanto è condizionata la validità del loro esercizio. Sul punto, si è anche detto che corrisponderebbe al significato lato o debole di "stato di diritto" in base al quale «ogni Stato deve essere uno stato di diritto, nel senso che ogni Stato è un ordinamento giuridico». Infatti, se si riconoscesse lo Stato come ordinamento giuridico, ogni Stato sarebbe uno stato di diritto e questo termine diviene pleonastico. Per tale osservazione, H. KELSEN, *La dottrina pura del diritto*, Torino, 1966, *passim*, spec. p. 345 e 351.

discrezionalità dei prestatori di servizio, che, purtuttavia, sopravvive con i nuovi strumenti.

Se ad ogni modo, oggi ci si affida alla *voluntary disclosure*, con le evidenti ricadute in tema di certezza del diritto e di garanzia dei diritti fondamentali, tanto vale armonizzare le discipline tra gli Stati e creare nuovi strumenti per la formazione della prova elettronica transfrontaliera.

L'affermazione potrebbe apparire semplicistica, ma è frutto di un percorso di ricerca che ha constatato come ad oggi non si possa fare a meno della formazione della prova elettronica transnazionale per la lotta alle gravi forme di criminalità, pena l'impossibilità di perseguire efficacemente i reati e di punire condotte gravemente riprovevoli.

In ciò si manifesta tutta l'elasticità del diritto. Il diritto è adattamento, il diritto è ente che segue la società e mai la precede, e pertanto, ad essa deve rispondere, ad essa deve adattarsi. Regolare una prassi diffusa significa – nel delicatissimo settore penalistico – colorare di legalità e di certezza attività ormai indispensabili nella società delle nuove tecnologie, ponendo al centro la libertà della persona e la tutela della collettività dalle forme di aggressione più gravi.

Il quadro legislativo e i meccanismi di cooperazione devono tenere il passo con i nuovi sviluppi della società e considerare che le nuove tecnologie donano nuove opportunità, ma anche nuove minacce, perché potrebbero essere usate per scopi malevoli.

La cooperazione volontaria ha sicuramente funzionato soprattutto nei rapporti con i prestatori di servizi aventi sede negli Stati Uniti d'America ed ha dato una prima risposta in un momento in cui gli Stati non erano ancora maturi abbastanza per formare norme coraggiose sulla formazione delle prove elettroniche. Ora, i tempi consentono di fare passi ulteriori.

Parlare di natura volontaria della cooperazione significa che la divulgazione è interamente a discrezione di un fornitore di servizi e non vi è alcuna prevedibilità. Infatti, il fornitore di servizi potrebbe fornire i dati necessari, fornirli solo parzialmente, decidere di non fornirli ovvero decidere quando fornirli. Inoltre, il fornitore di servizi potrebbe discrezionalmente decidere di notificare l'informazione sempre e comunque alla persona interessata, causando un possibile danno o compromettendo le indagini in corso.

Questa forma di cooperazione è lungi dall'essere soddisfacente, in quanto va a scapito della certezza del diritto e della responsabilità. A conferma di ciò, vi sono le relazioni sulla trasparenza pubblicate dai fornitori di servizi che non forniscono dettagli sufficienti riguardo all'esatta portata della loro cooperazione con gli attori della giustizia penale¹²⁹².

Concludendo, i nuovi strumenti per la formazione della prova elettronica transnazionale vanno verso una direzione ben precisa: principio di legalità e prevedibilità, nel tentativo di limitare la discrezionalità dei prestatori di servizi che, purtuttavia, non è eliminata, bensì sopravvive, seppur in margini più stringenti rispetto al passato.

Sullo sfondo, vi è un cambio di passo epocale nella cooperazione giudiziaria in materia penale: tutti i nuovi strumenti previsti dal Secondo protocollo, dal CLOUD Act e dalla proposta di Regolamento sugli ordini europei di produzione e di conservazione, pur non sostituendosi, ma affiancandosi ai vecchi strumenti rogatoriali, consentono una maggior efficacia applicativa perché abbandonano generalmente il classico rapporto tra

¹²⁹² Sul punto, C. BRIÈRE, *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, cit., p. 496; S. CARRERA, M. STEFAN, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, in *CEPS Paper*, Brussels, 2020, p. 22.

Stato di emissione e Stato di esecuzione, ovvero tra autorità, a favore di un rapporto diretto con privati aventi sede in un altro ordinamento giuridico.

È l'abbandono del principio di mutua assistenza. È l'evoluzione del principio del mutuo riconoscimento. È l'alba di un possibile nuovo terzo principio strutturale della cooperazione giudiziaria in materia penale. È la caduta del principio di territorialità, così come sinora conosciuto.

Invero, seppur esplicitamente basati sul principio del mutuo riconoscimento, così come sviluppati, gli ordini europei di conservazione e di produzione svilupperebbero meccanismi sensibilmente diversi rispetto a quelli classicamente previsti dal mutuo riconoscimento¹²⁹³. Si potrebbe paventare l'ipotesi di un terzo principio strutturale della cooperazione giudiziaria in materia penale, basato sull'interlocuzione diretta tra l'autorità giudiziaria dello Stato di emissione e un soggetto privato.

2. Le comuni e nuove incertezze

Sinora le fonti più importanti sono state la Convenzione sulla criminalità informatica e l'ordine europeo di indagine. Gli strumenti previsti hanno in qualche modo provato, per quanto possibile, a dare una risposta alle esigenze di legalità e alle istanze di sicurezza provenienti dalla collettività, garantendo la tutela dei diritti fondamentali. Oggi si può cominciare ad immaginare un nuovo scenario, fatto di nuovi strumenti previsti dal Secondo protocollo alla Convenzione sulla criminalità informatica, dal CLOUD Act statunitense e dal Regolamento sugli ordini europei di produzione e di conservazione.

Vanno posti dei quesiti, frutto di dubbi. Nonostante l'apprezzamento per i plurimi interventi e per gli sforzi compiuti ad ogni livello, bisognerebbe chiedersi se non si stia profilando una eccessiva stratificazione normativa che genererà incertezze applicative.

La proliferazione strumentale a cui si assiste rischia di donare alle autorità una serie di mezzi-fotocopia del tutto simili tra di loro, ma che non indicano in modo chiaro, preciso ed immediatamente percepibile quale sia lo strumento più adatto al caso concreto.

Un nodo centrale è la creazione di strumenti a più velocità, che renderebbero poco chiaro e coerente il quadro normativo.

Dalla normativa analizzata emerge che il metodo utilizzato per lo sviluppo dei nuovi strumenti per l'acquisizione di prove elettroniche all'estero sembra fare applicazione del principio di gradualità. Nell'applicare il principio di proporzionalità, ogni singolo strumento di ciascuna fonte normativa è stato immaginato come il prodotto di un delicato bilanciamento da una parte degli interessi della collettività e delle autorità proiettate ad ottenere nel minor tempo possibile informazioni estremamente volatili, dall'altra della tutela dei diritti fondamentali dei singoli, i quali avvertono i nuovi strumenti come particolarmente intrusivi della propria sfera intima e personale.

Questo sistema di pesi e contrappesi potrebbe rallentare ed appesantire le procedure. Gli adempimenti e le attività rischiano di risultare eccessivi e ridondanti, sino a smarrire l'interprete e l'operatore.

Chi dovrà utilizzare tali strumenti dovrà possedere una forte specializzazione ed avere una particolare ed approfondita conoscenza dell'ambito di applicazione e del settore specifico in cui opera. Dall'altra parte, anche i privati dovranno attrezzarsi con nuove

¹²⁹³ Concorde, sul punto, G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), cit., p. 1015.

figure professionali competenti in questo specifico settore, per rispondere alle richieste di assistenza, limitando gli errori ed evitando violazioni del diritto. Sarebbe, dunque, necessario garantire sistematicità. Di ciò potrebbe farsene carico l'Unione europea.

Orbene, sicuramente si assiste ad un rafforzamento della cooperazione in materia di criminalità informatica e della raccolta di prove di reato in formato elettronico a fini di indagini o processi penali.

È ormai ampiamente riconosciuta la necessità di una cooperazione rafforzata più efficace tra gli Stati e con il settore privato, nonché di una maggiore chiarezza e certezza del diritto per i prestatori di servizi e altri soggetti relativamente alle circostanze in cui possono rispondere alle richieste di divulgazione di prove elettroniche presentate dalle autorità giudiziarie penali di altri Stati.

Un ulteriore passo avanti verso una buona integrazione tra sistemi, da salutare con favore, è il riconoscimento da parte di tutte le fonti di nuova generazione che un'efficace cooperazione transfrontaliera tra autorità del settore pubblico e soggetti del settore privato richiede solide garanzie per la tutela dei diritti fondamentali¹²⁹⁴. È opportuno ritenere che quelle previste siano garanzie minime, potendo ogni singolo Stato innalzare il livello di tutela dei diritti fondamentali a favore dei singoli, senza però rendere inoperanti gli strumenti¹²⁹⁵.

A tal fine, tutte le nuove fonti seguono un approccio basato sulla garanzia dei diritti e prevedono condizioni e garanzie allineate con le fonti internazionali a tutela dei diritti umani.

Restano, però, perplessità sulla perseguibilità di tutti gli obiettivi a causa delle sovrapposizioni di disciplina che rischiano di rendere impraticabili gli obiettivi e di essere di intralcio nelle attività svolte. Ciò perché mancherebbe un approccio coraggioso e tempestivo da parte di tutti gli Stati ed un effettivo coordinamento internazionale solido.

Ad esempio, mentre il Secondo protocollo permetterebbe una cooperazione diretta con i prestatori di servizi solo nel caso in cui l'ordine abbia ad oggetto i nomi di dominio e i dati relativi agli abbonati, destinando alla mutua assistenza accelerata le richieste relative ad altre tipologie di dati, la proposta di Regolamento istituirebbe un sistema di cooperazione diretta per l'acquisizione di qualsiasi tipo di dato elettronico.

Se così è, allora il Secondo protocollo rischierebbe di diventare ben presto obsoleto e superato dalla normativa prevista per gli Stati membri dell'Unione europea, anche alla luce della possibilità di ottenere dati elettronici da prestatori di servizi che abbiano una sede in Paesi terzi ma che offrano servizi sul territorio dell'Unione europea.

Bisognerebbe comprendere che la criminalità informatica è realtà viva e fertile, così come l'uso delle nuove tecnologie. Non sembra più consentito rimandare la soluzione: il rischio è che ciò che può apparire nuovo ed efficace, con un'eccessiva riflessione, si tramuti in strumento vecchio, farraginoso e inefficiente. La tecnologia avanza, con essa la criminalità. Le risposte devono essere decise e celeri.

¹²⁹⁴ La dottrina ha già acutamente osservato come l'“intersezione necessaria” della tutela dei diritti dell'uomo sulla cooperazione giudiziaria in materia penale ha portato da tempo a una parziale “destatualizzazione” delle garanzie fondamentali chiamate a presiedere all'attuazione del mutuo riconoscimento delle decisioni giudiziarie, al percorso di ravvicinamento tra i sistemi penali e, più in generale, alla gestione unitaria dell'attività giurisdizionale. In tal senso, A. DI STASI, *Tutela multilevel dei diritti fondamentali e costruzione dello spazio europeo di giustizia*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale del titolo VI della Carta* (a cura di A. DI STASI), cit., p. 13 ss.

¹²⁹⁵ In tema, A. IERMANO, *Garanzie minime nello spazio europeo di giustizia penale*, Napoli, 2014, *passim*.

È rammaricante constatare come nel corso delle discussioni sul Secondo protocollo alla Convenzione sulla criminalità informatica alcune misure non siano confluite nel testo. Sebbene ritenute di grande interesse, a causa dei lavori supplementari che richiedevano, dei tempi e delle ulteriori consultazioni necessarie, sia le indagini sotto copertura per mezzo di un sistema informatico che l'estensione delle perquisizioni non sono stati ritenuti strumenti realizzabili in tempi brevi.

Pertanto, le Parti si sono riservate la possibilità di approntare nuovi strumenti in un prossimo futuro, pur nella consapevolezza che di una disciplina relativa a tali strumenti non se ne possa più fare a meno per un'efficace cooperazione giudiziaria in materia penale.

3. Sull'abbandono del principio di territorialità

Come è noto, l'attività di acquisizione extraterritoriale di dati elettronici collocati sul territorio di uno Stato diverso da quello al quale appartiene l'autorità procedente costituisce un'attività potenzialmente lesiva della sovranità territoriale dello Stato in cui i dati sono conservati¹²⁹⁶.

Si ritiene che, perché tale attività sia legittima, è necessario che vi sia un titolo legittimante, cioè una norma di diritto internazionale che la autorizzi, ossia una norma consuetudinaria, una disposizione convenzionale o, in assenza di queste, un'autorizzazione *ad hoc* di un soggetto idoneo ad impegnare sul piano internazionale lo Stato che deve subire l'acquisizione¹²⁹⁷.

Stando al principio di sovranità, l'ordinamento internazionale pone un generale divieto di ingerenza di uno Stato negli affari di altri Stati¹²⁹⁸. Il divieto comprende anche il *transborder data access*, secondo quanto emerge dal rapporto dell'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine¹²⁹⁹, dove è possibile constatare che due terzi dei Paesi del mondo concepiscano l'ordine di accesso ai sistemi informatici di altri Stati come inammissibile in assenza di specifica autorizzazione da parte dello Stato sovrano. Di conseguenza, non è possibile acquisire all'estero dati senza l'autorizzazione dello Stato dotato di sovranità territoriale¹³⁰⁰.

Sembra che il presupposto della centralità del ruolo del consenso del sovrano territoriale non sia sempre rispettato. Appare rispettato per il Secondo protocollo alla Convenzione sulla criminalità informatica perché il consenso dello Stato risulterà espresso in occasione della ratifica, la quale costituisce, dunque, il titolo di legittimazione

¹²⁹⁶ In argomento, G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, cit., p. 105 ss.

¹²⁹⁷ In tal senso, G.M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel transborder data access tra obblighi internazionali e norme interne di adattamento*, cit., p. 189.

¹²⁹⁸ Per uno studio sul principio di sovranità nell'area dell'Unione europea, A. DI STASI, *Parabola evolutiva della sovranità statale ed espansione delle competenze dell'Unione Europea: in particolare i limiti di applicabilità della Carta dei diritti fondamentali per gli Stati membri dell'Unione europea*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), Napoli, 2020, p. 185 ss.

¹²⁹⁹ Cfr., UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC), *Comprehensive Study on Cybercrime, Draft*, New York, 2013.

¹³⁰⁰ Sul punto, B.J. KOOPS, M. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, Tilburg, 2014, p. 35 ss., disponibile al link: https://repository.wodc.nl/bitstream/handle/20.500.12832/2047/2326-volledige-tekst_tcm28-73009.pdf?sequence=2&isAllowed=y.

internazionale dell'attività transfrontaliera e risulterà per l'Accordo esecutivo del CLOUD Act statunitense.

Tuttavia, il *Clarifying Lawful Overseas Use of Data Act* del 2018 attribuisce alle autorità statunitensi il potere di richiedere i dati archiviati dalla maggior parte dei principali fornitori di servizi di *cloud*, anche se conservati al di fuori degli Stati Uniti, senza una preventiva acquisizione del consenso del sovrano territoriale, tradendo così un approccio unilaterale sulla cui legittimità internazionale bisognerebbe riflettere.

Pare, inoltre, che non si sia scelto di individuare un presupposto agganciato al luogo in cui è conservato il dato, bensì al luogo in cui ha sede il prestatore di servizi che detiene il dato, o che vi abbia uno stabilimento o che abbia un criterio sostanziale con un determinato territorio valutato sulla base di specifici criteri di fatto.

Il consenso preventivo del sovrano richiamerebbe alla mente un approccio basato sul principio di territorialità¹³⁰¹, secondo cui la competenza relativa all'adozione i provvedimenti appartarrebbe all'autorità giurisdizionale dello Stato sul cui territorio si trovino i dati. Infatti, solamente con la previa acquisizione del consenso del sovrano territoriale sarebbe legittima l'acquisizione del dato elettronico da parte di un'autorità straniera. Tuttavia, secondo alcuni questo approccio non appare del tutto condivisibile¹³⁰².

Appare opportuno rilevare come sembri che lo sviluppo tecnologico mal si concili con i tradizionali principi giuridici come la territorialità. Un approccio basato sul principio di territorialità, incentrato essenzialmente sull'ubicazione del dato, appare poco pratico.

La crescita esponenziale di strumenti tecnologici come il *cloud computing* ha fatto emergere il superamento del principio di territorialità, se solo si tiene conto che i dati potrebbero essere trasferiti istantaneamente, in modo da non essere conservati in un unico *server*.

Restano, però, dubbi sui possibili conflitti di obblighi giuridici tra le varie giurisdizioni, questione di non poco conto e che le nuove fonti normative tentano di risolvere. Invero, la proposta di Regolamento sugli ordini europei di produzione e di conservazione introduce due strumenti obbligatori basati su una decisione che le autorità di emissione rivolgono ai fornitori di servizi ubicati in un altro Stato membro, in linea di principio senza coinvolgere l'altro Stato.

Il principio di territorialità basato sull'ubicazione del dato è sostituito da un nuovo sistema. Si istituirebbe in capo ai fornitori di servizi che prestano i propri servizi sul territorio dell'Unione europea l'obbligo di designare almeno un rappresentante legale in uno degli Stati membri dell'Unione europea per la ricezione, la valutazione e l'esecuzione degli ordini; mentre, in caso contrario, le autorità di emissione potrebbero inviare l'ordine a qualsiasi stabilimento del fornitore di servizi nell'Unione europea. Di conseguenza, l'effettiva ubicazione dei dati elettronici non assume rilevanza per decidere se la richiesta può essere emessa e in quale Stato debba essere indirizzata, anche se si tratti di uno Stato terzo.

Orbene, per evitare possibili conflitti di leggi, l'Unione europea dovrebbe procedere con un approccio globale e sistematico, individuando una disciplina armonica. Si

¹³⁰¹ Per uno studio del principio in relazione all'acquisizione di dati elettronici, G.M. RUOTOLO, Hey! You! Get Off My Cloud! *Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.*, 3, 2013, p. 785 ss.

¹³⁰² In dottrina, vi è chi ha sostenuto che l'accesso transfrontaliero ai dati in assenza dell'autorizzazione del sovrano territoriale è illegittima solo qualora dovesse arrecare danni materiali al sistema informatico all'estero o violare norme in materia di immunità. Cfr., V.H. VON HEINEGG, *Legal Implications of Territorial Sovereignty in Cyberspace*, in C. CZOSSECK, R. OTTIS, K. ZIOLKOSKI (eds.), *NATO 4th International Conference on Cyber Conflict*, 2012, Tallin, p. 7 ss.

dovrebbe procedere – invero, come sta già avvenendo – lavorando simultaneamente su tutte le fonti: proposta di Regolamento relativa agli ordini europei di produzione e conservazione, Accordo esecutivo con gli Stati Uniti d’America nell’ambito del CLOUD Act e Secondo protocollo alla Convenzione sulla criminalità informatica. Anche in questo caso, l’Unione europea si presenta come organismo di mediazione tra le varie posizioni, foriera di un dialogo e di un’armonica disciplina legislativa.

Evidenti, dunque, le ricadute: si sarebbe innanzi a un nuovo criterio di collegamento sostanziale, che individua lo Stato membro in cui il servizio è prestato. Il collegamento si considera esistente quando il fornitore di servizi ha uno stabilimento nell’Unione europea e, in assenza di tale stabilimento, quando sussistano criteri fattuali specifici, quali un numero significativo di utenti o la destinazione di attività in uno o più Stati membri, così come indicato all’art. 2 della proposta di Regolamento, aprendo così di fatto a prestatori di servizi aventi sede in Paesi terzi.

In conclusione, gli strumenti tenderebbero ad una extraterritorialità dello Stato membro emittente che può obbligare un prestatore di servizi situato nel territorio di un altro Stato a fornire le informazioni necessarie per un’indagine giudiziaria.

4. Il ruolo propulsivo dell’Unione europea: un’ambizione possibile

Come indicato nella strategia dell’UE del 2020 per l’Unione della sicurezza¹³⁰³, nella strategia dell’UE del 2020 in materia di cbersicurezza per il decennio digitale¹³⁰⁴ e nella strategia dell’UE del 2021 per la lotta alla criminalità organizzata¹³⁰⁵, la Commissione si è impegnata a concludere in modo rapido ed efficace i negoziati sul Secondo protocollo alla Convenzione sulla criminalità informatica. Il Parlamento europeo ha, d’altra parte, riconosciuto la necessità di concludere i lavori sul protocollo nella sua risoluzione del 2021 sulla strategia dell’UE in materia di cbersicurezza per il decennio digitale.

La Commissione ha inoltre partecipato, a nome dell’Unione europea, ai negoziati sul protocollo in linea con la decisione del Consiglio dell’Unione europea e si è consultata costantemente con la Commissione speciale del Consiglio per i negoziati in merito alla posizione dell’Unione.

La presenza della Commissione dell’Unione europea ha avuto un notevole impatto sui risultati. Il ruolo dell’Unione europea come osservatore garantisce omogeneità e l’assenza di obblighi confliggenti. È chiaro che l’Unione europea può candidarsi ad essere motore propulsore di un cambiamento. Con la sua funzione di stimolo potrà garantire la sistematicità degli strumenti.

L’Unione europea potrà assicurare il coordinamento e potrà dare un decisivo contributo al chiarimento del diritto applicabile.

¹³⁰³ Cfr., Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla strategia dell’UE per l’Unione della sicurezza, 24 luglio 2020, COM(2020) 605 final.

¹³⁰⁴ Cfr., Comunicazione congiunta al Parlamento europeo e al Consiglio la strategia dell’UE in materia di cbersicurezza per il decennio digitale, 16 dicembre 2020, JOIN(2020) 18 final.

¹³⁰⁵ Cfr., Parere del Comitato economico e sociale europeo sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Strategia dell’UE per la lotta alla criminalità organizzata 2021-2025, 22 settembre 2021, COM(2021) 170 final.

La *voluntary disclosure* e le norme unilateralmente emanate presentano diversi svantaggi, tra cui la frammentazione ed il rischio di violazione della legge di un altro Stato.

Per rimediare alla “parcellizzazione” delle norme che permettono alle autorità pubbliche di chiedere direttamente ai fornitori di servizi di conservare e divulgare le prove elettroniche, è necessario un chiarimento della legge applicabile. Tale chiarimento comporta non solo l’elaborazione di norme comuni o almeno compatibili, ma anche l’adozione di norme che affrontino i conflitti di legge. Gli strumenti di nuova generazione vanno verso questa direzione. I dubbi sorgono quando si analizza il modo in cui tali chiarimenti vengono forniti.

Il ruolo dell’Unione europea dovrà consistere nello sforzo di creare coesione e sistematicità, mediante un’operazione volta al chiarimento. Il processo è basato sul raggiungimento di tre obiettivi simultanei tra di loro interconnessi.

Un primo obiettivo consta nell’elaborazione di norme applicabili ai fornitori di servizi che operano all’interno dell’Unione europea, al fine di garantire l’applicazione di standard uniformi. Ciò sarà possibile con il Regolamento sugli ordini europei di produzione e di conservazione.

Un secondo obiettivo si è avuto con la negoziazione di norme multilaterali, finalizzate a fornire standard minimi comuni. Tuttavia, bisognerebbe verificare nel tempo se saranno garantiti gli standard proposti in sede di redazione del Secondo protocollo addizionale alla Convenzione sulla criminalità informatica. Sarà inoltre necessario verificare come i due sistemi si integreranno.

Infine, un terzo obiettivo da raggiungere consiste nella negoziazione di un accordo bilaterale con gli Stati Uniti, nell’ambito di quanto stabilito dal CLOUD Act. Questo accordo completerebbe gli standard internazionali, affrontando più specificamente gli obblighi potenzialmente conflittuali tra le leggi dell’Unione europea e degli Stati Uniti d’America nonché fornendo regole più specifiche, per esempio sulle autorità competenti per la richiesta di prove. Le istituzioni dell’Unione europea partecipano a questi tre processi simultanei che interagiscono tra loro e difendono interessi specifici in ciascuno di essi.

La sua posizione di osservatore privilegiato le consente di poter agire con tempestività e di seguire da vera protagonista l’evoluzione normativa. Sarà, quindi, compito della Commissione europea – e dell’Unione europea tutta – assicurare che le fonti normative relative alla formazione delle prove elettroniche nazionali siano tra di loro compatibili, evitando gli obblighi contrastanti e tentando di aumentare le garanzie minime a tutela dei diritti fondamentali.

L’azione mediatrice dell’Unione europea potrà essere la vera chiave di volta nell’individuazione di una strada metodologicamente comune che possa garantire i futuri standard globali, individuando un minimo comune denominatore tra le varie discipline che possa fungere da fondamento per possibili future soluzioni a problematiche che, realisticamente, non mancheranno. Sarà l’esperienza e l’applicazione concreta ad indicare le aree di intervento bisognose di operazioni volte a perfezionare il sistema delle procedure per la formazione delle prove elettroniche transnazionali.

La visione globale di cui dovrà tener conto l’Unione europea sarà di fatto punto nodale per ribadire l’importanza a tutti i livelli di una sufficiente protezione dei diritti fondamentali coinvolti nelle operazioni di acquisizione dei dati informatici aventi attitudine probatoria in un processo penale.

Le ontologiche diversità presenti all'interno ed all'esterno dell'Unione europea dovranno trovare un punto di sintesi adeguato in regole procedurali armoniche in tutti gli ordinamenti, al fine di rendere effettivi ed efficaci gli strumenti per la formazione delle prove elettroniche.

Sarà, dunque, necessario prevenire eventuali sovrapposizioni normative e, laddove non possibile, individuare strumenti di compensazione che non blocchino le procedure, pena il fallimento degli strumenti di nuova generazione per la formazione dell'*e-evidence*.

Sarà, poi, essenziale garantire la certezza del diritto e l'accessibilità agli strumenti. Per realizzare ciò, è di fondamentale importanza evitare che gli operatori del diritto e i fornitori di servizi siano colti impreparati da questa rivoluzione.

Per rispondere ad esigenze di efficacia, questi strumenti avranno bisogno anche di una ristrutturazione e di una nuova organizzazione delle autorità giudiziarie e degli uffici del settore privato. Sarà necessario prevedere la formazione del personale afferente alle autorità giudiziarie, al fine di offrire le conoscenze necessarie, utili per un tempestivo utilizzo dei nuovi strumenti per la formazione delle prove elettroniche transnazionali.

Ristrutturazione, riorganizzazione e formazione sono le condizioni di effettività per il corretto impiego dei nuovi strumenti. Condizioni di effettività che risultano indispensabili alla luce della proliferazione normativa e dell'evidente implementazione di un elevato numero di strumenti, talvolta con discipline differenziate in base al tipo di dato da richiedere.

Non è una visione efficientistica. Bisogna riflettere sulla concreta ed ordinata applicazione degli strumenti per evitare il fallimento di essi. Se è vero, come dimostrato, che l'85% delle indagini penali oggi richiede l'ausilio di strumenti per la produzione di dati informatici e che per due terzi di queste indagini vi è la necessità di ottenere tali prove da prestatori di servizi online con sede in un altro ordinamento, allora vuol dire che una buona organizzazione degli uffici e una buona conoscenza delle fonti internazionali e sovranazionali non solo renderà il sistema più efficiente, ma favorirà la qualità delle indagini e del processo, con evidenti ricadute sulla qualità delle decisioni, prodotti finali dell'accertamento della verità processuale. Anche da qui passano le garanzie del giusto processo, anche da qui passa la tutela dei diritti fondamentali.

Gli strumenti dovranno poi garantire tempi ragionevoli, costi accettabili, armonico impiego delle risorse.

Anche i fornitori di servizi dovranno reinventarsi, prevedendo al loro interno tecnici competenti e formati per questo tipo di attività. Accanto ai timori di un'eccessiva discrezionalità del privato nelle decisioni relative alla conservazione e produzione dei dati elettronici, si affianca l'effettiva garanzia del principio di legalità di cui sono portatrici le nuove fonti normative.

Sebbene il coinvolgimento diretto del privato ad oggi non sembra eliminabile, è pur sempre possibile richiedere una preparazione specifica nel nuovo settore, con figure adeguatamente formate e che possano beneficiare di sistemi informatici all'avanguardia per la valutazione delle richieste e per la trasmissione dei dati elettronici.

A tal proposito, è auspicabile che in futuro possano beneficiare anche i privati di piattaforme da cui trarre esperienze acquisite da altri organi sulle stesse questioni o su questioni simili, al fine di agevolare la circolazione delle informazioni e l'efficienza delle procedure, con evidenti benefiche ricadute sull'economia processuale. In tal modo, si renderebbero disponibili le informazioni e gli arresti giurisprudenziali relativi all'interpretazione del diritto dei Paesi terzi e alle procedure di conflitto degli Stati membri.

Ad oggi, come già indicato nel lavoro, si è pensato di coinvolgere unicamente gli organi giurisdizionali creando una apposita sezione dedicata su una piattaforma centrale quale il progetto SIRIUS e/o la Rete giudiziaria europea.

5. Secondo protocollo addizionale alla Convenzione sulla criminalità informatica e attività dell'Unione europea

L'Unione europea ha avuto un ruolo centrale nella stesura del Secondo protocollo addizionale relativo alla cooperazione rafforzata e la divulgazione di prove elettroniche.

Invero, nell'ambito del mandato di negoziazione conferito dal Consiglio dell'Unione europea il 6 giugno 2019, la Commissione europea ha partecipato ai lavori, a nome degli Stati parte della Convenzione e contestualmente membri dell'Unione europea, assicurando un notevole impegno confluito, poi, nei risultati.

In particolare, potendo contare su una visione globale, da osservatore privilegiato ha potuto consigliare di porre una particolare attenzione al rispetto dei diritti fondamentali e dei principi generali del diritto dell'Unione europea quali sanciti nei Trattati e nella Carta dei diritti fondamentali dell'Unione europea.

Invero, come constatato, anche il Secondo protocollo segue un approccio basato sui diritti, con condizioni e garanzie specifiche, alcune delle quali sono inserite nell'ambito delle peculiari misure di cooperazione, nonché nel capo III del protocollo.

L'attività svolta dalla Commissione europea è coerente con gli obiettivi e con i valori fondanti l'Unione stessa. Va, infatti, sottolineato come tutti gli Stati membri dell'UE facciano parte anche del Consiglio d'Europa e come questi si siano impegnati a proteggere un livello minimo di garanzie per i diritti fondamentali. Inoltre, la materia oggetto dal Secondo protocollo è in gran parte disciplinata da norme comuni basate sull'art. 82, par. 1, e sull'art. 16 TFUE.

Nel partecipare ai negoziati a nome dell'Unione europea, la Commissione si è accertata che il protocollo fosse pienamente compatibile con il diritto dell'Unione europea e con gli obblighi che ne derivano per gli Stati membri, verificando che le disposizioni del Protocollo consentiranno agli Stati membri di rispettare i diritti fondamentali.

Ulteriore compito è stata la verifica di compatibilità delle disposizioni del Protocollo con la proposta di Regolamento relativa agli ordini europei di produzione e di conservazione, in modo tale da evidenziare eventuali conflitti di legge. Tale attività non può dirsi del tutto conclusa. Restano questioni aperte soprattutto relative alla proposta di Regolamento che dovranno essere risolte.

In virtù del ruolo assunto dall'Unione europea, in vista dell'apertura alla firma del Secondo Protocollo e delle ratifiche che ne conseguiranno, la Commissione ha formulato una proposta di decisione che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il Secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche¹³⁰⁶ e presenterà in futuro anche una proposta di decisione del Consiglio dell'Unione europea che autorizza gli Stati membri a ratificare il protocollo nell'interesse dell'Unione europea. In tal modo, conferma il suo ruolo centrale, volto al progresso ed

¹³⁰⁶ Proposta di decisione del Consiglio che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche, Bruxelles, 25 novembre 2021, COM(2021) 718 final.

all'agevolazione di rapporti fecondi e produttivi con gli altri ordinamenti a qualsiasi livello.

Con la sua attività partecipativa ai negoziati, l'Unione europea ha garantito la compatibilità del Secondo protocollo con le pertinenti norme dell'Unione europea. Pertanto, nel voler perseguire l'obiettivo di armonizzazione delle discipline, evitando per quanto possibile eventuali conflitti di legge, con l'art. 2 della proposta di decisione ad oggetto sembrerebbe vincolare gli Stati membri alla formulazione di riserve, dichiarazioni, notifiche e comunicazioni, così come figureranno nell'apposito allegato.

Dunque, con la decisione si consente agli Stati di adottare un approccio uniforme a talune riserve e dichiarazioni, notifiche e comunicazioni, al fine di garantire la compatibilità dell'attuazione del Secondo protocollo con il diritto dell'Unione europea.

In particolare, risulta di fondamentale importanza prevedere una disciplina uniforme tra gli Stati membri che consenta alla nuova Procura europea di poter agire nel pieno delle proprie potenzialità investigative.

Ed invero, gli Stati membri che partecipano alla cooperazione rafforzata istituita dal Regolamento (UE) 2017/1939 relativo all'istituzione della Procura europea ("EPPO"), dovranno includere l'EPPO, nell'esercizio delle sue competenze di cui agli artt. 22, 23 e 25 di tale Regolamento, tra le autorità oggetto della comunicazione di cui all'art. 8, par. 10, lett. a) e b), del Secondo protocollo¹³⁰⁷.

Inoltre, gli Stati membri che partecipano alla cooperazione rafforzata istituita dal Regolamento (UE) 2017/1939 relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea ("EPPO"), dovranno garantire che l'EPPO, nell'esercizio delle sue competenze di cui agli artt. 22, 23 e 25 di tale Regolamento, possa chiedere la cooperazione a norma del protocollo allo stesso modo dei procuratori nazionali di tali Stati membri.

È importante sottolineare come tale scelta avrà evidenti ricadute sui futuri rapporti tra Unione europea e Consiglio d'Europa. Infatti, il Consiglio d'Europa e l'Unione europea condividono gli stessi valori fondamentali – diritti umani, democrazia e stato di diritto – ma sono organismi internazionali distinti, con ruoli diversi, seppur complementari.

6. La vera “sfida” dell'Unione europea: l'efficienza degli ordini europei di produzione e di conservazione

Una sfida importante per l'Unione europea è l'elaborazione degli ordini europei di produzione e di conservazione. La creazione dei due strumenti rappresenta una delle priorità stabilite dalla Commissione perché ritenuti essenziali per un'efficace cooperazione in materia penale, grazie all'istituzione di un meccanismo efficiente ed affidabile che prevede strutture e garanzie chiare per l'acquisizione di prove elettroniche.

Come già chiarito, attualmente la proposta è in fase di “trilogo politico”. In altre parole, è stata avviata una discussione sulle proposte presentate al fine di fare sintesi ed individuare un testo comune che possa soddisfare gli interessi di tutte le parti politiche chiamate a sviluppare gli strumenti.

¹³⁰⁷ Secondo l'art. 8, par. 10, lett. a) e b), del Secondo protocollo, all'atto della firma del protocollo o del deposito del proprio strumento di ratifica, accettazione o approvazione, ciascuna Parte deve comunicare al Segretario generale del Consiglio d'Europa e aggiornare i dati di contatto delle autorità designate per emettere un ordine e per ricevere un ordine in conformità dell'art. 8 del Secondo protocollo.

I progressi sinora fatti al fine di individuare un testo condiviso sono importanti. Emerge, tuttavia, una particolarità. Il vero ago della bilancia non sembra essere il principio di proporzionalità – pur sempre elemento centrale dello strumento – bensì la fiducia reciproca.

Infatti, è in relazione al grado di fiducia reciproca ritenuto acquisito tra gli Stati membri che potrà individuarsi un soddisfacente testo di compromesso. Più sarà alto il livello di fiducia reciproca percepito dagli attori politici, meno saranno gravosi gli adempimenti che saranno previsti per emettere ed eseguire gli ordini, e viceversa.

Il testo proposto dal Consiglio con il suo orientamento generale sembra già individuare un bagaglio di adempimenti di non poco conto, con la previsione di complessi meccanismi di rifiuto e di subprocedimenti che spaziano dalla convalida *ex ante* del provvedimento, ai motivi di rifiuto, alla procedura aggravata a seguito di inottemperanza prevista all'art. 14 della Proposta di Regolamento, passando per il complesso meccanismo di notifica previsto all'art. 7-*bis* ed al meccanismo di “consultazione preventiva” di cui all'art. 5, par. 7, della proposta di Regolamento, sino ad arrivare ad un ineliminabile diritto al ricorso effettivo, previsto all'art. 17 della proposta di Regolamento, che pur dovrebbe essere garantito a tutte le persone interessate dall'ordine di produzione, e non solo a coloro i cui dati sono stati ricercati, come invece attualmente la proposta prevede.

Ulteriore riflessione è sulle tempistiche. Alle petizioni di principio che vogliono strumenti rapidi per la conservazione e la produzione delle prove elettroniche e che impongono tempi contingentati per la produzione ridotti sino a sei ore dalla ricezione del certificato, si contrappongono una serie di adempimenti precedenti e successivi all'emissione che appesantiscono il procedimento e che rischiano di diventare la regola, pur essendo previsti sovente come eccezioni.

Solo per fare un esempio, potrebbe farsi un abuso dei casi di inottemperanza, per fini “difensivi” da parte dei prestatori di servizi, qualora vi siano incertezze relative alla disciplina applicabile, compulsando così l'attivazione della procedura aggravata di cui all'art. 14 della proposta di Regolamento da parte dell'autorità di emissione. In questo modo, il provvedimento di riconoscimento emesso all'esito della procedura diventerebbe un sicuro “scudo” per i detentori dei dati, che neutralizzerebbero così il rischio di violazione di altre norme. Tale pratica potrebbe far assumere allo strumento le caratteristiche di un ordine europeo di indagine, con conseguente perdita delle peculiarità originarie ed allungamento dei tempi di acquisizione.

Orbene, si tratta di notazioni dubitative che auspicano l'apertura di un dibattito fecondo, nella piena consapevolezza che solo l'applicazione concreta potrà far emergere possibili falle nel sistema.

La principale sfida è legata alla necessità di trovare un equilibrio tra, da un lato, la garanzia di un meccanismo efficace per l'acquisizione di prove elettroniche in materia penale e, dall'altro, la salvaguardia dei diritti fondamentali delle persone i cui dati sono ricercati, tenendo pienamente conto del principio di fiducia reciproca.

Dunque, il meccanismo di tutela dei diritti fondamentali sarà proiezione del livello di fiducia reciproca che si riterrà raggiunto. È al variare di questo livello che cambierebbero le modalità di emissione ed esecuzione degli strumenti.

Uno dei banchi di prova sembrerebbe essere il regime di notifica. Se presupposto è un alto livello di fiducia reciproca, allora il Regolamento potrà prevedere che lo Stato di emissione debba avere la responsabilità principale di garantire un giusto processo e di salvaguardare i diritti fondamentali di qualsiasi persona i cui dati siano stati ricercati mediante ordine.

Viceversa, se non si riterrà sussistente un livello adeguato di fiducia reciproca, sarà conferito allo Stato di esecuzione il potere sostanziale di vigilare su tutti gli ordini indirizzati a un prestatore di servizi o a un rappresentante legale stanziato sul proprio territorio.

Tuttavia, in tale ultimo caso, dovrebbe considerarsi l'impatto che gli oneri amministrativi potrebbero generare sullo Stato di esecuzione. Gli adempimenti rischierebbero di essere ingestibili perché lo Stato dovrà compiere una valutazione per ogni ordine ricevuto. In secondo luogo, l'ordine potrebbe rivelarsi poco innovativo rispetto agli attuali strumenti esistenti o addirittura poco efficiente rispetto alla *voluntary disclosure*. Una possibile soluzione di compromesso potrebbe essere un meccanismo di notifiche periodiche in blocco e la previsione di un obbligo di notificazione per alcuni ordini secondo una periodicità adeguata¹³⁰⁸.

Il regime delle notificazioni, poi, non sembrerebbe ragionevole per gli ordini europei di conservazione. Ciò perché si tratta di uno strumento scarsamente afflittivo e assolutamente non idoneo a diffondere dati elettronici, per cui non sembra vi sia alcuna necessità di individuare particolari meccanismi di compensazione a carattere informativo, dal momento in cui i dati non sono rivelati ad alcuno.

Diversamente, per gli ordini europei di produzione le notificazioni sono molteplici e variano, appunto, al mutare del livello di fiducia reciproca percepito dai decisori politici. I punti critici sono essenzialmente tre: per quali tipi di dati garantire la notificazione, quale valore assume la notificazione, chi dovrà provvedere a notificare.

Se da una parte vi è chi ritiene necessario garantire una notificazione qualora sia richiesto qualsiasi tipo di dato, dall'altro c'è chi considera ragionevole e proporzionato eseguire una notificazione qualora siano richiesti i dati relativi al contenuto, estendendole al massimo anche ai dati relativi alle operazioni¹³⁰⁹.

Ulteriore considerazione è relativa alla funzione che debba assumere la notificazione: si spazia dalla mera funzione informativa sino a ricomprenderla tra i motivi di rifiuto, con evidenti effetti sul regime di acquisizione ed utilizzabilità del dato informatico.

Tra l'altro, bisognerebbe riflettere sulla concreta funzione che andrebbe ad assumere una notifica fatta solo per informazione e quali conseguenze essa possa manifestare sul piano concreto.

Si potrebbe immaginare un doppio binario anche per le notifiche: da una parte, i dati relativi agli abbonati ed agli accessi, per cui non dovrebbe essere prevista alcuna notifica o una notifica al solo scopo informativo; dall'altra, i dati relativi alle operazioni ed al contenuto, per cui dovrebbe essere prevista una notifica soltanto qualora la persona i cui dati siano richiesti sia residente in uno Stato diverso da quello i cui dati sono richiesti e per cui la mancata notifica potrebbe essere un motivo di rifiuto.

Tuttavia, anche queste soluzioni non sembrano improntate alla semplificazione delle procedure ed all'acquisizione di un maggior livello di fiducia reciproca.

Sistematicamente, non appare opportuno, infine, attribuire un effetto sospensivo alla notifica, al fine di non allungare ulteriormente i tempi.

¹³⁰⁸ Si potrebbe pensare ad una periodicità di tre mesi, sei mesi o un anno.

¹³⁰⁹ Il regime delle notificazioni è il tema di maggior rilevanza nella fase delle trattative in sede di triloquio. Alle posizioni dei rappresentanti del Parlamento europeo, che richiedono un ampliamento del regime delle notificazioni, si contrappongono le posizioni dei rappresentanti del Consiglio che, nell'operare delle aperture, ritiene comunque non oberare gli operatori di adempimenti eccessivi e ritenuti poco ragionevoli.

Non va taciuto, inoltre, come la fiducia reciproca è un bene di cui c'è immensamente bisogno in un mondo globalizzato ed esposto a imponenti rischi ed attacchi da parte della criminalità organizzata e del terrorismo¹³¹⁰. È l'unione e la coesione dei popoli e degli ordinamenti statuali che può aiutare a realizzare un'efficace lotta alle moderne forme di criminalità, poste sociologicamente al di fuori degli ordinamenti giuridici.

Ulteriori riflessioni dovrebbero essere compiute sui motivi di rifiuto. Bisognerebbe chiedersi se in aggiunta agli attuali motivi di rifiuto, non sia necessario inserirne di nuovi, magari facoltativi. In tal caso, potrebbe fare da contrappeso l'inserimento di un obbligo di consultazione dell'autorità di emissione prima di sollevare un motivo di rifiuto al fine di scongiurare la stasi della fase di esecuzione o l'allungamento dei tempi. Anche qui, decisivo sarà il livello di fiducia reciproca che si riterrà raggiunto.

Orbene, la valutazione relativa al livello di fiducia reciproca acquisito è squisitamente politica, pertanto esula dalla valutazione dell'interprete, che in questo momento può solamente limitarsi a farsi "vate" ed indicare le possibili strade percorribili che vadano nella direzione della creazione dei nuovi strumenti e non dell'abbandono di una proposta che appare allo stato dell'arte meritevole.

Ulteriore notazione a carattere sistematico è relativa alla necessità di lavorare simultaneamente e contemporaneamente su più fonti, in modo da rendere armonico l'impianto normativo relativo all'acquisizione delle prove elettroniche all'estero. Un'Unione europea efficiente ed attenta ai diritti fondamentali non può sottrarsi al delicato compito di operare una normazione del mondo digitale compiendo scelte equilibrate e coerenti che abbiano una visione globale del tema e che affrontino le questioni dettando principi a carattere sistematico.

E pertanto, non può il legislatore europeo esimersi dal tener conto di tutte le proposte normative in tema di nuove tecnologie, *internet*, *cloud* ed *internet service provider*¹³¹¹.

Soluzioni efficaci ai problemi posti sono tutt'ora possibili, purché non siano a scapito di uno strumento bilanciato ed efficiente. Al contrario, si limiterebbe notevolmente l'applicazione pratica dello strumento, sino al punto di minare lo stesso principio della fiducia reciproca in questo settore.

È necessario bilanciare tutti gli interessi in gioco nell'ambito non solo dell'ordine interno ma anche delle relazioni interordinamentali¹³¹². Si tratta di trovare un equilibrio

¹³¹⁰ Per un'analisi relativa all'evoluzione delle condotte dei gruppi terroristici nel tempo, V. LOIA, F. ORCIULLI, *Understanding the composition and evolution of terrorist group networks: A rough set approach*, in *Future Generation Computer Systems*, 101, 2019, p. 983 ss.

¹³¹¹ In particolare, il legislatore europeo dovrà tenere in considerazione, ad esempio, quanto stabilito nel Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, relativo al contrasto della diffusione di contenuti terroristici online, in GUUE n. L 172 del 17 maggio 2021; mentre, dall'altra parte, dovrà garantire la sistematicità delle normative di riferimento, creando una disciplina equilibrata e coerente con altre proposte quali, ad esempio, la proposta di Regolamento del Parlamento e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM/2020/825 final e la proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final.

¹³¹² Sul punto, si è osservato che la tecnica del bilanciamento «prende forma e si fa apprezzare non soltanto nel "chiuso" dell'ordine interno ma si proietta pure – grazie proprio al principio di apertura – al piano delle relazioni interordinamentali. L'operatore è, infatti, naturalmente sollecitato a volgere lo sguardo *anche* fuori della finestra costituzionale aperta sul mondo esterno, a trattare le norme *aliunde* prodotte che si immettano con le forme prescritte in ambito interno e in esso spieghino i loro effetti al pari delle norme che in quest'ultimo vengono a formazione, interrogandosi ogni volta in merito a quale di esse possa maggiormente giovare alla soluzione del caso, vale a dire a concorrere a fissare il più in alto possibile il

che sia di garanzia per l'efficienza e l'innovatività dei nuovi strumenti e che concili gli interessi dello Stato di emissione e quelli dello Stato di esecuzione con la protezione dei diritti della persona interessata. Sul punto, è opportuno considerare – tra le altre cose – che la persona interessata potrebbe essere residente in uno Stato diverso da quello di emissione e di esecuzione. In tale caso, saranno coinvolti anche gli interessi e le tutele di un Paese terzo. Qui rilevante sarà una nuova concezione del principio di territorialità o un abbandono di esso, almeno quando il tema è relativo alla formazione delle prove elettroniche.

7. Ampliamento del diritto di difesa *versus* limitazione delle investigazioni difensive

Una delle tematiche più sentite, perché coinvolge direttamente il diritto di difesa, è la possibilità per il difensore di svolgere nell'ambito del proprio mandato attività difensive a carattere investigativo nell'ambito del sistema di cooperazione.

Invero, il tema in dottrina è stato ampiamente discusso, in relazione ai classici sistemi rogatoriali ed alle prospettive di innovazione apportate dagli ordini europei di indagine¹³¹³. Resta, dunque, da appurare se, col tempo, siano possibili o siano state fatte aperture ed innovazioni in tema di investigazioni all'estero coordinate dai difensori.

In particolare, la disciplina prevista per il tradizionale sistema rogatorio basato sulla mutua assistenza non consente alla difesa una richiesta diretta di rogatoria all'autorità estera¹³¹⁴. Tuttavia, siccome una radicale posizione sul punto rischierebbe di creare una lesione del diritto alla prova, la giurisprudenza ha riconosciuto al difensore la facoltà di promuovere istanza all'ufficio del pubblico ministero o al giudice per le indagini preliminari affinché costoro attivino la procedura della rogatoria internazionale¹³¹⁵.

punto di sintesi assiologica, quello cioè nel quale la Costituzione come “sistema” di valori fondamentali positivizzati si afferma ed appaga nel modo migliore in relazione alle complessive esigenze del caso stesso». Così, A. RUGGERI, *L'equilibrio nei rapporti tra Corti europee e Corti nazionali: un'autentica quadratura del cerchio possibile solo in prospettiva de iure condendo*, in *Rivista Freedom, Security & Justice: European Legal Studies*, 3, 2021, p. 13.

¹³¹³ In argomento, M. CAGOSI, *Un illustre assente: la vittima del reato nell'ordine europeo di indagine penale*, cit., p. 119 ss.; M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, cit., p. 7 ss.; A. CIAMPI, *L'assunzione di prove all'estero in materia penale*, Milano, 2003; D. CIMADOMO, *Ordine europeo di indagine e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, cit., p. 224 ss.; A. CISTERNA, *Un passo importante per omologare le investigazioni Ue*, in *Guida al diritto*, 40, 2017, p. 39; R. PICCIRILLO, *I profili funzionali e strutturali dell'Ordine europeo di indagine penale*, cit., p. 60 ss.; P. SPAGNOLO, *Il procedimento di emissione dell'OEI*, cit., p. 86 ss.; M. TROGU, sub art. 31, *Ordine europeo di indagine penale*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018, p. 1082 ss.

¹³¹⁴ In tal senso, P. SPAGNOLO, *Il procedimento di emissione dell'OEI*, cit., p. 87 ss.

¹³¹⁵ Cfr., Cass., sez. I, 29 maggio 2007, n. 23967, in *Cass. pen.*, 12, 2008, p. 4707 ss., secondo cui «in relazione alla inutilizzabilità delle investigazioni difensive deve rilevarsi che la stessa discende dai principi generali del codice di procedura penale e, pur non essendo esplicitamente affermato che il difensore non può recarsi all'estero a svolgere dette investigazioni, discende dall'ordinamento tale divieto, essendo evidente che, ai fini dell'utilizzabilità di atti compiuti all'estero, per tutte le parti processuali, deve essere esperita la procedura prevista dal codice in materia di rogatorie. Poiché non è prevista la possibilità per il difensore di ricorrere alla rogatoria all'estero, ne discende che tale tipo di atto non è esperibile dal difensore mediante la disciplina prevista dall'art. 391 bis c.p.p. ed egli ha l'obbligo di passare attraverso la richiesta al P.M. o al GIP, affinché costoro attivino la procedura della rogatoria internazionale. D'altronde, tramite le indagini difensive non è esperibile ogni tipo di atto: il legislatore ha limitato l'oggetto delle indagini

Una apertura, in una visione evolutiva, sembrava esserci stata con l'ordine europeo di indagine. Invero, l'art. 1, par. 3, della direttiva 2014/41/UE, attribuisce all'indagato e al difensore la legittimazione ad agire per l'emissione di un ordine di indagine, al fine di garantire il diritto di difesa.

L'art. 31, d.lgs. 21 giugno 2017, n. 108, restituisce un'interpretazione restrittiva. Nel colmare le lacune del precedente sistema rogatorio, si limita a prevedere espressamente il potere del difensore di richiedere all'autorità competente l'emissione di un ordine europeo di indagine, individuando espressamente tra i legittimati il difensore della persona sottoposta alle indagini, dell'imputato e della persona per la quale è stata proposta l'applicazione di una misura di prevenzione¹³¹⁶.

Sono esclusi, in quanto non espressamente individuati, i difensori delle altre parti private, della persona offesa e del terzo titolare del bene, il che comporta evidenti ripercussioni negative su un'effettiva parità delle armi, perché un legittimo potere non è riconosciuto in capo a determinati difensori, in primo luogo quelli delle persone offese¹³¹⁷. La scelta, invero di politica legislativa, non appare logicamente, sistematicamente e assiologicamente spiegabile.

Le fonti di nuova generazione relative all'acquisizione di dati elettronici all'estero, pur facendo riferimento al diritto di difesa, non menzionano mai il difensore o l'avvocato né fanno alcun riferimento esplicito alle attività difensive a vocazione investigativa che egli può compiere nell'ambito del mandato conferitogli. Questo lascerebbe intendere che anche per le fonti di nuova generazione sia necessaria un'attività di canalizzazione della richiesta nei confronti dell'autorità di emissione, secondo quanto previsto dalla giurisprudenza.

Simile impostazione è stata ritenuta condivisibile nell'ambito della cooperazione giudiziaria, così come sinora conosciuta con gli strumenti classici, ove la richiesta di assistenza è prerogativa delle autorità giudiziarie individuate dai singoli Stati e che possono comunicare direttamente tra loro. Tutto questo regge l'impianto sistematico, dal momento in cui si applica il principio di territorialità.

Tuttavia, le fonti di nuova generazione stabiliscono un rapporto diretto tra autorità di emissione e prestatore di servizi, con una conseguente comunicazione diretta pubblico/privato. Si sarebbe di fronte a una radicale evoluzione nei rapporti di cooperazione giudiziaria relativa all'acquisizione dei dati elettronici.

Orbene, una lettura sistematica tra gli strumenti di vecchia e nuova generazione dovrebbe condurre alla conclusione che, nel voler applicare i nuovi strumenti, sia comunque necessaria una richiesta canalizzata all'autorità di emissione, la quale provvederà a vagliarla, senza però applicare parametri definiti, in quanto non sono

all'assunzione di dichiarazioni, alla richiesta di documentazione, all'accesso ai luoghi, ma ad esempio non ha previsto la possibilità di effettuare accertamenti tecnici irripetibili, in relazione ai quali il difensore ha l'obbligo di inoltrare richiesta al P.M.». Per un commento alla sentenza, F. ALBANO, *Sui limiti territoriali delle indagini difensive: note a margine di una discutibile pronuncia*, cit., p. 4707 ss.; C. ANGELONI, *L'inammissibilità di investigazioni difensive all'estero: una ricostruzione plausibile?*, cit., p. 1383 ss.; M. BORDIERI, *Brevi note sull'inutilizzabilità di atti di investigazione svolti all'estero dal difensore dell'imputato senza passare attraverso una rogatoria internazionale*, cit., p. 2035 ss.; D. CURTOTTI NAPPI, *I nuovi orizzonti investigativi del difensore: le informazioni assunte all'estero*, cit., p. 986 ss.

¹³¹⁶ Così, A. CISTERNA, *Un passo importante per omologare le investigazioni Ue*, cit., p. 39; P. SPAGNOLO, *Il procedimento di emissione dell'OEI*, cit., p. 88.

¹³¹⁷ Critici sul punto, M. CAGOSI, *Un illustre assente: la vittima del reato nell'ordine europeo di indagine penale*, cit., p. 119 ss.; D. CIMADOMO, *Ordine europeo di indagine e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, cit., p. 224.

previste espressamente le ragioni che possono determinare il rigetto¹³¹⁸ e lasciando, dunque, un ampio margine di discrezionalità in capo all'organo che procede.

Così come descritta, questa soluzione potrebbe comportare una limitazione eccessiva del diritto alla prova, data dalla localizzazione territoriale del dato elettronico, laddove il diritto non dovrebbe subire compressioni dovute allo spazio o al territorio¹³¹⁹. Senonché, per un corretto approccio alla problematica, bisognerebbe tener in debita considerazione la costruzione del sistema e verificare se da una lettura globale garantista dei diritti fondamentali, non ci siano margini di manovra per un intervento diretto e fattivo del difensore, evidenziando momenti di frizione e di opportunità evoluzionistiche.

Una apertura sul punto sicuramente è fatta dall'art. 234-*bis* c.p.p.¹³²⁰, di chiara derivazione internazionale perché rappresenta l'adattamento interno dell'art. 32 della Convenzione sulla criminalità informatica. Sebbene la dottrina si sia concentrata sul comprendere chi fosse il legittimo titolare dei dati informatici che dovrebbe prestare il consenso all'apprensione del dato (tema a cui una risposta è stata data nel capitolo dedicato alla Convenzione sulla criminalità informatica) bisognerebbe considerare anche che la norma può fungere da apripista per l'intervento attivo del difensore nello svolgimento delle attività investigative all'estero relative a dati informatici, senza passare attraverso il sistema di canalizzazione dell'istanza all'autorità pubblica.

La norma consente siffatta attività diretta unicamente qualora il dato sia disponibile al pubblico o previo consenso del legittimo titolare. Tuttavia, alla luce del rapporto diretto che si instaura tra autorità pubblica e privato previsto con i nuovi strumenti, bisognerebbe riflettere se vi siano spazi di manovra che consentano, a seguito di un intervento legislativo, anche al difensore di poter interloquire direttamente con gli *internet service provider* senza dover canalizzare la richiesta.

Le riflessioni dovrebbero concentrarsi su due attività diverse in relazione al soggetto a cui si riferiscono i dati: l'attività investigativa del difensore relativa ai dati che si riconducibili al proprio assistito e l'attività investigativa relativa ai dati nei confronti di terzi. La distinzione appare necessaria perché diverse sono le sensibilità da tener conto nello sviluppare una normativa garante dei diritti fondamentali.

Una soluzione univoca alla questione di certo non è possibile rinvenirla in questo momento storico. Ciò che invece appare ragionevolmente certa è la disparità di trattamento a cui va incontro il difensore rispetto alle possibilità investigativo-probatorie che si stanno dischiudendo nei confronti delle autorità di contrasto o degli organi investigativi ed inquirenti.

La strada da percorrere è sicuramente difficile, ricca di dubbi ed insidie. Ma è innegabile che un sistema equilibrato di pesi e contrappesi, basato sul principio di legalità e su una procedura garante della riservatezza e magari custodita da organi terzi ed imparziali che fungano da presidi di controllo e garanzia dei diritti fondamentali, può essere un percorso virtuoso, per raggiungere una piena parità delle armi tra le diverse parti

¹³¹⁸ Sugli aspetti critici, in relazione agli classici di assistenza giudiziaria, P. SPAGNOLO, *Il procedimento di emissione dell'OEI*, cit., p. 89.

¹³¹⁹ Sul diritto alla prova, G. VASSALLI, *Il diritto alla prova nel processo penale*, in *Riv. It. Dir. proc. pen.*, 1968, p. 12.

¹³²⁰ L'apertura nei confronti del difensore sarebbe possibile perché l'acquisizione è resa agevole dal fatto che gli elementi sono reperibili nelle reti informatiche, e possono perlopiù essere raccolti a distanza senza l'assistenza tecnica di un'autorità giudiziaria straniera. Sui profili relativi all'utilizzabilità, M. DANIELE, *La sfera d'uso delle prove raccolte*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018, p. 195.

che si trovano a duellare in quello splendido ed al tempo stesso tremendo gioco¹³²¹, quale è il procedimento penale, anche di matrice europea, e della cooperazione in materia penale.

8. Tecnologia e diritti fondamentali. A lezione dai classici per possibili azioni bilanciate

Kafka scrisse che di Prometeo si narrano quattro leggende.

Gli antichi greci raccontavano che Prometeo – il titano più intelligente di tutta la mitologia, emblema della curiosità e personificazione dell'ingegno umano – è punito da Zeus perché, per rendere gli uomini più forti, ha donato loro il fuoco, simbolo delle formidabili armi del progresso.

Nel Protagora, anche Platone riprende il mito. Il filosofo racconta che Prometeo e il fratello Epimeteo si incaricarono di distribuire le varie qualità tra gli esseri viventi. Le doti dovevano essere distribuite in modo che ogni specie fosse in grado di sopravvivere. Ma Epimeteo sbagliò nella distribuzione e l'umanità, rimasta per ultima, ne rimase sprovvista. Allora Prometeo, dopo aver rubato con un inganno il fuoco ad Atena, lo donò agli uomini, permettendo loro di sopravvivere e progredire.

Nel celebre Prometeo incatenato, Eschilo racconta che Zeus, per vendicarsi dell'inganno subito, inflisse al titano una tremenda punizione. Dopo averlo condotto nella Scizia remota ed inospitale, i fedeli servitori del padre degli Dèi, Kràtos (Potere) e Bìa (Forza), incatenarono Prometeo ad una rupe del Caucaso. Zeus, dal par suo, inviava ogni giorno un'aquila perché gli squarciasse il petto e gli dilaniasse il fegato, che gli ricresceva durante la notte.

Nella mitologia classica, Zeus, col passare del tempo, da tiranno selvaggio e feroce si trasformò in un campione di giustizia. Infatti, dal racconto del Protagora si evince che con il dono del fuoco, gli uomini sapevano come procurarsi da vivere, ma ignoravano ancora le tecniche di costruzione delle città ed erano in balia delle bestie selvagge. Più tardi, quando si riunirono per far fronte agli attacchi, non fecero altro che litigare tra loro. Zeus, allora, cercò di far sì che sopravvivessero e mandò loro Ermes con coloro che sedevano accanto al suo trono: Aidòs (Rispetto) e Díke (Giustizia). Sia Aidòs sia Díke vennero distribuite fra gli uomini ugualmente¹³²².

Il mito ben si presta a descrivere icasticamente l'attuale rapporto tra nuove tecnologie e diritti fondamentali. Da esso ben si può trarre giovamento per sperimentare e proporre nuovi scenari in tema di acquisizione di elementi elettronici transfrontalieri aventi attitudine probatoria.

Invero, è necessario che la società ed i diversi saperi dialoghino con il mondo del diritto, fornendo spunti, mettendo in evidenza problemi ancora irrisolti e proponendo soluzioni, nella consapevolezza che «risulta molto più importante capire che sapere, avere un'intelligenza critica dei problemi piuttosto che apprendere tecnicismi e procedure» e «cogliere quanto profonde siano le interconnessioni tra il modo di intendere la giustizia e il modo di vivere la democrazia»¹³²³.

¹³²¹ Cfr., P. CALAMANDREI, *Il processo come giuoco*, Milano, 1950, *passim*.

¹³²² Cfr., H. LLOYD-JONES, *Il Prometeo incatenato*, in AA.VV., *Fortuna critica degli autori greci* (a cura di U. ALBINI, F. BORNHANN, M. NALDINI), Firenze, 1977, p. 87.

¹³²³ V., G. GIOSTRA, *Prima lezione sulla giustizia penale*, Bari-Roma, 2020, p. IX ss.

Il mito ben evidenzia il conflitto sorto tra il progresso scientifico, rappresentato da Prometeo, ed il concetto di autorità nonché l'essenza dei diritti fondamentali, impersonificati da Zeus.

Una delle grandi sfide contemporanee è quella di individuare il punto di corretto equilibrio tra le libertà di cui è motore il regno di internet e i diritti fondamentali da proteggere anche nel territorio virtuale.

Il dibattito in dottrina ed in giurisprudenza diventa sempre più acceso, complice uno sviluppo incredibilmente veloce delle nuove tecnologie, che ha posto al centro il dilemma della “tutela della persona nell'uso delle tecnologie digitali”.

È evidentemente che da qui bisogna partire per individuare un percorso virtuoso che sia di sintesi tra l'auspicata efficienza delle indagini digitali all'estero ed il rispetto dei diritti di coloro che ne sono interessati.

Un assioma è che l'accesso ad internet non può essere accompagnato da una perdita dei diritti. Diversamente, l'utente diventerebbe una sorta di “vittima consapevole”, titolare della scelta di collocarsi in una sfera meno garantita¹³²⁴.

Di questo, il mito dona una lettura chiara: una volta venuti in possesso del fuoco, delle “nuove tecnologie”, gli uomini non ne sono stati più privati, né sono stati limitati nella loro condizione. Anzi, tutt'altro, perché Zeus ha inviato loro, in uno dei momenti bui, gli “strumenti” per ben operare. Ha inviato loro la Giustizia.

È dal senso di Giustizia, dalla figlia di Zeus, dai diritti fondamentali che bisogna partire per un'analisi futura che vuole indicare in che modo siano migliorabili gli strumenti descritti in questo studio. Qui ci si è limitati a mettere in evidenza solo alcuni dei tanti aspetti problematici ed a proporre delle possibili soluzioni, guardando al tema con la “lente d'ingrandimento” dei diritti fondamentali e della dignità umana.

Del resto, per affrontare le prossime, eventuali sfide relative all'acquisizione delle prove elettroniche transnazionali «è utile partire dalla individuazione dei diritti inviolabili della persona, così come configurati a seguito di una lettura delle Carte dei diritti “orientata” alla luce della giurisprudenza sovranazionale e costituzionale»¹³²⁵.

Nel verificare “sul campo” il funzionamento dei nuovi strumenti e nel tracciare i futuri aspetti problematici che immancabilmente si verificheranno, sarà di fondamentale importanza trarre insegnamenti fecondi e propositivi dall'esperienza concreta e porre, poi, nuovi profili di sperimentazione con coraggio, pazienza e prudenza¹³²⁶, nella consapevolezza che solo dal dialogo tra il mondo del diritto e il mondo dell'informatica potranno nascere le soluzioni adeguate.

Per funzionare, gli strumenti per l'acquisizione di prove elettroniche all'estero non hanno bisogno solo di una disciplina chiara, precisa ed incondizionata, ma anche di un'infrastruttura digitale efficiente. Strumenti nuovi, così diversi da quelli del passato a cui i giuristi sono abituati, hanno bisogno di organizzazione, risorse e di strumenti informatici funzionanti ed all'avanguardia. L'attuale sistema è fatto di strumenti in parte obsoleti, dall'impatto negativo sul raggiungimento degli obiettivi. Per cui è necessaria una riorganizzazione e la garanzia di un perfetto funzionamento.

¹³²⁴ In tal senso, L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018, Milano, 2019, p. 206; S. RODOTÀ, *Il mondo nella rete. Quali vincoli, quali diritti*, cit., p. 28.

¹³²⁵ Così, L. KALB, *Introduzione*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018, cit., p. 18.

¹³²⁶ Cfr., M. CARTABIA, L. VIOLANTE, *Conflitti tragici, conflitti giuridici*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), cit., p. 130.

Sul punto, va salutato con favore lo sforzo che sta compiendo il Consiglio d'Europa e l'Unione europea. Starà poi ai singoli Stati raccogliere la sfida: riuscire a garantire l'effettivo funzionamento degli strumenti di comunicazione per lo scambio di informazioni e prove elettroniche.

Anche nel settore della cooperazione giudiziaria in materia penale e, per quanto di interesse in questo lavoro, dell'acquisizione degli elementi informatici a fini probatori, è necessario evitare che i principi che permeano la società europea ed occidentale siano ridotti a vuota retorica, applicando un solido realismo ed una pragmatica concretezza.

Bisognerà capire come bilanciare l'impatto dei nuovi strumenti con i valori nascenti¹³²⁷ che si originano in questo nuovo settore, prendendo le mosse dalla tutela della dignità umana – vero ago della bilancia – e del libero sviluppo della personalità¹³²⁸.

In particolare, si assiste a un difficile rapporto tra il diritto all'informazione, il diritto alla privacy e la tutela dei dati personali, i quali, secondo la dottrina, devono «trovare un nuovo punto di equilibrio nella salvaguardia dell'identità personale del soggetto nella sua proiezione sociale»¹³²⁹.

Internet e ciò che esso rappresenta non è né un male né un bene, così come non lo è Prometeo. Tuttavia, come osservato all'inizio di questo lavoro, c'è sempre del bene e del male in tutte le cose create dall'uomo, semplicemente perché imperfette. Stesso approccio per gli strumenti che vogliono combattere la criminalità o che si avvalgono delle nuove tecnologie. Gli strumenti del Secondo protocollo alla Convenzione sulla criminalità informatica, la disciplina del CLOUD Act, gli ordini europei di produzione e di conservazione non sono né da valutare negativamente, né da considerare perfetti.

Probabilmente si poteva fare meglio, probabilmente la complessità dei vari sub-procedimenti o il numero eccessivo di strumenti crea incertezze. Ciò che innegabilmente risulta positivo è la chiara e netta presa di posizione nel ritenere il principio di legalità una garanzia ineludibile¹³³⁰. Ciò è tanto più chiaro, quanto più si nota come gli strumenti

¹³²⁷ Di recente, la Corte europea dei diritti dell'uomo si è pronunciata su un caso austriaco stabilendo che sebbene l'anonimato degli utenti su internet non sia un diritto assoluto, le autorità nazionali, prima di ordinare l'esecuzione di una misura relativa alla divulgazione dei dati personali degli utenti, devono effettuare un bilanciamento tra i diritti e gli interessi in gioco. Cfr., Corte EDU, 7 dicembre 2021, *Standard Verlagsgesellschaft MBH v. Austria* (no. 3), causa n. 39378/15.

¹³²⁸ Il riferimento è al diritto di autodeterminazione informativa, al diritto alla garanzia dell'integrità e della riservatezza dei sistemi informatici ed al nucleo essenziale della vita privata. I tre aspetti realizzano «una sorta di “prosecuzione” virtuale della tutela dell'individuo, resa necessaria dal fatto che ciascuno tede oramai ad esprimere gran parte della propria personalità proprio attraverso il sistema informatico». In tal senso, L. PARLATO, *Libertà della persona nell'uso delle tecnologie digitali*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale, Salerno, 25-27 ottobre 2018, cit., p. 227 ss. V., inoltre, D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, cit., p. 74. La dottrina ha osservato che a seguito dello sviluppo tecnologico, sono emerse dalla coscienza sociale dei “nuovi diritti”, i quali, sebbene non godano di un esplicito riconoscimento normativo, hanno acquisito un importante “tono costituzionale” che li collocano all'interno della costituzione in modo implicito. Così, T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, cit., p. 465.

¹³²⁹ Così, A. MARANDOLA, *La tutela dell'identità personale (informatica), anche del soggetto coinvolto in un processo penale*, cit., p. 375.

¹³³⁰ Secondo la dottrina, «i percorsi sono tutti governati dalla legge, anzi spesso dalla sua più alta espressione, quella della tassatività, secondo il principio di ordine generale che tiene unito il sistema, cioè, il principio di ragionevolezza. Invero, una materia come quella penale, coinvolgente i rapporti tra autorità ed individuo e sotto questo profilo i diritti di libertà non può non essere governata dalla riserva di legge, che fissa le situazioni di illiceità, regola i poteri dell'accusa e della difesa, affida – con le c.d. finestre di giurisdizione – al giudice i poteri decisorii relativi». Così, G. SPANGHER, *Introduzione allo studio del processo penale*, cit., p. 69.

abbiano la vocazione a soppiantare i rapporti basati sulla collaborazione volontaria instaurati sinora tra autorità pubbliche e privati detentori dei dati.

È dal principio di legalità che bisognerà ripartire per capire se è possibile individuare e quale potrà essere l'eventuale regime di utilizzabilità delle prove elettroniche raccolte all'estero¹³³¹.

Sicuramente è difficile coniugare le plurime esigenze. Individuare un equilibrio di certo non è facile. Come osservato, il contingentamento dei tempi, necessaria risposta alla volatilità dei dati elettronici, spesso mal si concilia con la sovrapposizione degli adempimenti e dei controlli. Dall'altra parte, però, questi ultimi sembrano necessari per garantire i diritti fondamentali, secondo il principio di proporzionalità e di ragionevolezza.

Una risposta a tali conflitti dovrà darla la politica, con lo strumento dell'accordo, nella consapevolezza che solamente il confronto e il dialogo schietto e sincero su un argomento così delicato può portare alla soluzione dei problemi¹³³².

A questo compito non potranno sottrarsi – ed invero, non lo stanno facendo – le corti ed i tribunali, tra cui la Corte europea dei diritti dell'uomo, la Corte di giustizia dell'Unione europea e le Corti costituzionali nazionali, il cui compito è quello di comporre i conflitti alla luce del diritto¹³³³.

È pur vero che spesso il diritto non fornisce risposte chiare e condivise, ma è anche vero che a dilemmi relativi a un mondo – come quello di internet – ancora poco noto a chi non ha competenze specifiche e settoriali una risposta dovrà esser data il più presto possibile, per evitare che la criminalità trovi un terreno dove guadagnare l'impunità (non solo commettendo *cybercrime* ma anche reati di matrice "classica") e, di conseguenza, far cadere nel baratro il mondo del digitale, così come avviene per Prometeo alla fine della tragedia eschiliana.

¹³³¹ La dottrina ha evidenziato come le sanzioni processuali siano poste a presidio del valore etico-sociale della giustizia istituzionale perché «dimostrano che l'ordinamento – dopo aver elaborato il miglior percorso per cercare di raggiungere la verità e comunque per far sì che la collettività accetti *pro veritate* la decisione cui si perviene al termine dello stesso – non è disposto ad accontentarsi di strade alternative, evidentemente scartate perché ritenute meno affidabili. Considerare irrilevante ogni deviazione dal modello legale risulterebbe senz'altro "economicamente" più conveniente, ma significherebbe rassegnarsi a giudicare senza aver dato fondo alle migliori regole conosciute per rendere giustizia». Sul punto, G. GIOSTRA, *Prima lezione sulla giustizia penale*, cit., p. 11.

Siffatta impostazione, trasportata nell'ambito dell'acquisizione delle prove elettroniche transnazionali, sembra schiudere nuovi scenari d'indagine che coinvolgono il rapporto tra gli strumenti legali per la formazione delle prove elettroniche all'estero e l'uso del captatore informatico per attività di perquisizione *on-line*. Appare chiaro che le attività di perquisizione ed acquisizione di dati elettronici con lo strumento del captatore informatico sia maggiormente invasivo, non esistendo ad oggi una disciplina settoriale e soprattutto non riuscendo a garantire la genuinità del dato. Tutto ciò non sembra verificarsi con i nuovi strumenti che, seppur operano solo in relazione a dati transfrontalieri, riescono a garantire la genuinità delle informazioni, potendo la società privata detentrica del dato apporre dei sigilli di autenticità al documento e garantirne l'immodificabilità.

¹³³² In dottrina si è affermato che nelle operazioni di bilanciamento, la tappa cruciale è rappresentata dal principio di proporzionalità in senso stretto, che appartiene al campo dei giudizi di valore e come tale ha carattere essenzialmente politico. Il principio tollera scostamenti e approssimazioni entro certi limiti intorno alla linea direttrice. In tal senso, D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, cit., p. 64.

¹³³³ In dottrina, si è autorevolmente sostenuto che il carattere pervasivo delle pronunce della Corte europea dei diritti dell'uomo e della Corte di giustizia dell'Unione europea «non solo impattano sul caso concreto, ma entrano a pieno titolo nell'ordinamento nazionale». Cfr., A. MARANDOLA, *Introduzione*, in AA.VV., *Speciale CEDU e ordinamento interno*, Dir. pen. e proc., Milano, 2014, p. 4 ss.

È dall'accordo e dal confronto per far sintesi che bisognerà ripartire individuando il corretto punto di equilibrio tra i vari interessi in gioco. È seguendo questa linea che ciascuno sacrifica l'integrità della propria pretesa, uscendone, tuttavia, tutti vincitori e più coesi.

Questo lo sapevano bene Zeus e Prometeo. Inserendosi nel solco della tradizione, Zeus perviene ad un accordo con il demiurgo degli esseri umani. Zeus rinuncia all'oltranzosa protervia del suo dominio; Prometeo accetta di riconoscere la nuova giustizia che il dio porta nel mondo¹³³⁴. È vero che Zeus – quel senso di autorità e di rispetto per i diritti umani – non altera la sua natura ed invia Dike agli uomini per avvantaggiarsene, ma è anche vero che Prometeo – il progresso tecnologico – può sforzarsi quanto vuole di creare spazi di libertà in cui è possibile agire impunemente ma, per quanta simpatia egli abbia potuto ispirare agli animi generosi dei liberali come Shelley, rimane pur sempre una figura minore nel Pantheon greco. È Zeus che regge l'universo. Sono la dignità umana ed i diritti fondamentali gli organi-motore di un armonico progresso, che non devono mai invecchiare, ma evolversi sempre¹³³⁵.

Va compiuto uno sforzo di disponibilità per trovare una disciplina specifica più armonica nel settore delle prove informatiche, coniugando il passato con il futuro. Passato e futuro devono incontrarsi per collaborare, procedendo per tentativi ed immaginazione. Solo insieme le istituzioni nazionali, sovranazionali e internazionali con gli operatori del diritto, il modo dell'accademia e gli altri *stakeholders* potranno individuare la soluzione alle problematiche fatte emergere in questo lavoro e le cui soluzioni sono state abbozzate solo in parte, nella consapevolezza che una soluzione univoca non possa esistere.

Dunque, passato e futuro che si incontrano, Zeus e Prometeo, tradizione ed innovazione insieme per rispondere alle nuove esigenze volte alla coesione sociale¹³³⁶. Da un lato, il passato dovrà aver fiducia del futuro e consigliare la strada migliore da intraprendere, dall'altro il futuro avrà l'arduo compito di innovare, nel solco della tradizione, senza disperdere le conquiste ottenute, facendo ordine nel caos, nella consapevolezza che – per dirla con Gustav Mahler – «tradizione non è culto delle ceneri, ma custodia del fuoco».

È stato questo il filo conduttore del lavoro: fare ordine, tra passato e futuro, in un sistema di fonti caotico e, dopo ciò, individuare alcuni punti problematici (presenti e futuri) in un mondo del tutto nuovo ed a tratti inesplorato, con un metodo deduttivo, alla cui base è stato posto l'empirismo e il falsificazionismo. Su quali saranno gli approdi futuri, di certo non vi è certezza. Sono tanti i possibili epiloghi.

¹³³⁴ Per tale lettura, D. DEL CORNO, *Introduzione a ESCHILO, Supplici, Prometeo incatenato*, Milano, 1994, p. XIV.

¹³³⁵ Sul tema, vi è chi ha osservato che «i diritti fondamentali e gli altri principi di giustizia costituzionalmente stabiliti si sono affermati come limiti e vincoli a tutti i poteri e, insieme, come la ragione sociale dell'intero artificio istituzionale, da essi finalizzato alla loro garanzia». Cfr., L. FERRAJOLI, *La costruzione della democrazia. Teoria del garantismo costituzionale*, cit., p. 121.

¹³³⁶ Sul punto, M. CARTABIA, L. VIOLANTE, *Le leggi cambiano, la loro interpretazione evolve*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), cit., p. 133 ss., secondo cui «per essere fedele a se stesso, l'ordinamento deve recare in sé un'apertura e una spinta alla trasformazione, perché il diritto positivo è essenzialmente espressione storica di una determinata comunità politica. È risposta a bisogni che mutano nel tempo. È ricerca di un ordine e di una coesione sociale che deve continuamente riscoprirsi. È reazione a sfide future mutevoli e sempre nuove. Dalla sua relatività scaturisce il suo carattere intrinsecamente dinamico: le leggi cambiano, la loro interpretazione evolve, le loro potenzialità applicative sono aperte a implicazioni sempre nuove. La legge è un corpo vivente: esso preserva la sua identità anche se la singola cellula che lo compone è soggetta a un incessante processo di cambiamento, di decadenza e di rinnovamento».

Questo era chiaro anche a Kafka che, dopo aver letto probabilmente Cicerone e le Odi di Pindaro, annotò le quattro leggende di Prometeo.

Secondo la prima, poiché aveva svelato i segreti degli dèi agli uomini, fu incatenato ad una roccia del Caucaso e gli dèi mandavano aquile a divorargli il fegato, che sempre ricresceva.

Nella seconda, durante la sua agonia, per il dolore dei colpi di becco, Prometeo si strinse sempre più alla roccia finché diventò un tutt'uno con essa.

Secondo la terza, nel corso dei millenni il suo tradimento fu dimenticato. Gli dèi dimenticarono, le aquile dimenticarono, egli stesso dimenticò.

Secondo la quarta, ci si stancò di lui che non aveva più ragione di essere. Gli dèi si stancarono, le aquile si stancarono, e la ferita, stanca, si richiuse.

Rimane solo l'inspiegabile montagna di roccia.

La leggenda tenta di spiegare l'inspiegabile. Dal momento che proviene da un fondo di verità, deve finire di nuovo nel regno dell'inspiegabile.

Tuttavia, è quel fondo di verità – a cui il diritto deve tendere – che consente di continuare nel sano progresso sociale e civile e che non bisogna dimenticare se si vuole coltivare la conoscenza da porre al servizio della società, perché «i miti ci avvertono che trastullarci con il sapere e sfruttarlo sono azioni pericolose, ma che l'uomo deve e vuole conoscere, e che una volta impadronitosi della conoscenza non la dimenticherà»¹³³⁷.

¹³³⁷ D.S. LANDES, *Prometeo liberato. La rivoluzione industriale in Europa dal 1750 a oggi*, Torino, 2000, p. 732.

BIBLIOGRAFIA

- AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007;
- AA.VV., *Lo spazio di libertà, sicurezza e giustizia* (a cura di U. DRAETTA, N. PARISI, D. RINOLDI), Napoli, 2007;
- AA.VV., *Manuale delle investigazioni sulla scena del crimine. Norme, tecniche, scienze* (a cura di D. CURTOTTI, L. SARAVO), Torino, 2013;
- AA.VV., *Carta dei Diritti Fondamentali dell'Unione Europea* (a cura di R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI), Milano, 2017;
- AA.VV., *La Carta dei diritti fondamentali dell'Unione europea. Efficacia ed effettività* (a cura di V. PICCONE, O. POLLICINO), Napoli, 2018;
- AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- H.H. ABRAHA, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, in *International Data Privacy Law*, 3, 2019, p. 207 ss.;
- H.H. ABRAHA, *Regulating Law Enforcement Access to Electronic Evidence Across Borders: the United States Approach*, in *Information & Communication Technology Law*, 3, 2020, p. 324 ss.;
- H.H. ABRAHA, *Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiative*, in *International Journal of Law and information Technology*, 29, 2021, p. 118 ss.;
- D. ACHILLE, *Primato del diritto europeo e tutela dei diritti fondamentali nel sistema ordinamentale integrato*, in *Nuova giur. civ.*, 12, 2018, p. 1890 ss.;
- R. ADAM, *La cooperazione nel campo della giustizia e affari interni: da Schengen a Maastricht*, in *Rivista di diritto europeo*, 1994, p. 225 ss.;
- R. ADAM, *La cooperazione in materia di giustizia e affari interni tra comunitarizzazione e metodo intergovernativo*, in *DUE*, 2/3, 1998, p. 481 ss.;
- F.C. AETERTON, *Teledemocracy. Can technology protect democracy?*, Newbury Park, 1987;
- AGENZIA PER L'ITALIA DIGITALE, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, in www.archivio.digitpa.gov.it, 2012;
- R. AGO, *Droit des traités à la lumière de la Convention de Vienne*, in *Collected Courses of the Hague Academy of International Law*, 3, 1971, p. 303 ss.;
- A. AL-RAWI, *Video Games, Terrorism, and ISIS's Jihad 3.0*, in *Terrorism and Political Violence*, 4, 2018, p. 740 ss.;
- F. ALBANO, *Sui limiti territoriali delle indagini difensive: note a margine di una discutibile pronuncia*, in *Cass. pen.*, 12, 2008, p. 4707B ss.;

- T. A. ALEINIKOFF, *Constitutional Law in the Age of Balancing*, in *Yale Law Journal*, 96, 1987, p. 943 ss.;
- T. ALESCI, *La Procura europea per i reati lesivi di interessi finanziari: la proposta di regolamento tra luci e ombre*, in *Arch. Pen.*, 1, 2014, p. 1 ss.;
- M. ALFIERI, *Giudice naturale*, in *Dig. disc. pen.*, V, Torino, 1991;
- L. ALGERI, *L'esame del minore al vaglio della Consulta: la mobilità del giudice naturale preserva la concentrazione*, in *Dir. pen. proc.*, 12, 2018, p. 1565 ss.;
- A. ALÌ, *La risposta della Comunità internazionale al fenomeno dei Foreign Terrorist Fighters*, in *La Comunità int.*, 2, 2015, p. 181 ss.;
- S. ALLEGREZZA, *Pubblico ministero e azione penale: stato dell'arte e prospettive di sviluppo*, in AA.VV., *Profili del processo penale nella Costituzione europea* (a cura di M. G. COPPETTA), Torino, 2005;
- S. ALLEGREZZA, *Cooperazione giudiziaria, mutuo riconoscimento e circolazione della prova penale nello Spazio giudiziario europeo*, in AA.VV., *L'area di libertà sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007;
- S. ALLEGREZZA, *L'armonizzazione della prova penale alla luce del Trattato di Lisbona*, in *Cass. pen.*, 10, 2008, p. 3882 ss.;
- S. ALLEGREZZA, *Critical remarks on the Green paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9, 2010, p. 569 ss.;
- S. ALLEGREZZA, *Collecting Criminal Evidence Across the European Union: the European Investigation Order Between Flexibility and Proportionality*, in AA.VV., *Transnational Evidence in Multicultural Inquiries* (a cura di S. RUGGERI), Heidelberg, 2014;
- S. ALLEGREZZA, A. MOSNA, *Cross-Border Criminal Evidence and the Future European Public Prosecutor. One Step Back on Mutual Recognition?*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018;
- S. ALLEGREZZA, A. MOSNA, F. NICOLICCHIA, *L'acquisizione della prova all'estero e i profili transnazionali*, in AA.VV., *Diritto penale delle società* (a cura di G. CANZIO, L.D. CERQUA, L. LUPARIA), Padova, 2016;
- P. ALLISON, A. HINDOCHA, *US Global Cybercrime Cooperation: A Brief Explainer*, in *Third Way*, 26 giugno 2020;
- F. ALONZI, *L'escalation dei mezzi di intrusione nella sfera privata: ripartire dalla Costituzione*, in *Rev. Bras. de Dereito Processual Penal*, 3, 2019, p. 1421 ss.;
- V. ALTAMORE, *"Mandato di arresto europeo" e "diritti fondamentali": dall'assolutezza alla negoziabilità dei diritti fondamentali? Spunti di riflessione in una recente sentenza della Corte di giustizia*, in *Diritto pubblico comparato ed europeo*, 2013, p. 602 ss.;
- C. AMALFITANO, *Conflitti di giurisdizione e riconoscimento delle decisioni penali nell'Unione Europea*, Milano, 2006;
- C. AMALFITANO, *Spazio giudiziario europeo e libera circolazione delle decisioni penali*, in *Studi sull'integrazione europea*, 1, 2009, p. 73 ss.;
- C. AMALFITANO, *L'azione dell'Unione Europea per la tutela delle vittime di reato*, in *Il Diritto dell'Unione europea*, 2011, p. 643 ss.;

- C. AMALFITANO, *Mandato d'arresto europeo: reciproco riconoscimento vs diritti fondamentali? Note a margine delle sentenze Radu e Melloni della Corte di giustizia*, in *penalecontemporaneo.it*, 4 luglio 2013;
- C. AMALFITANO, sub Art. 82 TFUE, in AA.VV., *Trattati dell'Unione Europea* (a cura di A. TIZZANO), II ediz., Milano, 2014;
- C. AMALFITANO, *Unione europea e principio del reciproco riconoscimento delle decisioni penali*, in AA.VV., *L'ordine europeo di protezione. La tutela delle vittime di reato come motore della cooperazione giudiziaria* (a cura di H. BELLUTA, M. CERESA GASTALDO), Torino, 2016;
- K. AMBOS, *European Criminal Law*, Cambridge, 2018;
- E. AMODIO, *Diritto di difesa e diritto alla prova nello spazio giudiziario europeo*, in AA.VV., *Il difensore e il Pubblico Ministero europeo* (a cura di A. LANZI, F. RUGGIERI, L. CAMALDO), Padova, 2002;
- E. AMODIO, *Il processo penale tra disgregazione e recupero del sistema*, in *Verso la riscoperta di un modello processuale. Convegno in memoria di Antonino Galati*, Atti del Convegno. Caserta, 12-14 ottobre 2001, Milano, 2003;
- E. AMODIO, *Il diritto delle prove penali nel pensiero di Mirjan Damaška*, in *Riv. it. dir. e proc. pen.*, 1, 2007;
- E. AMODIO, *Il processo come gioco tra letteratura e diritto vivente*, in *Riv. It. Dir. e Proc. Pen.*, 4, 2020, p. 1664 ss.;
- C. ANGELONI, *L'inammissibilità di investigazioni difensive all'estero: una ricostruzione plausibile?*, in *Riv. it. dir. e proc. pen.*, 3, 2008, p. 1384 ss.;
- E. ANODINA, *Cooperazione-integrazione penale nell'Unione europea*, in *Cass. pen.*, 10, 2001, p. 2898 ss.;
- E. ANDOLINA, *Il potere del difensore di acquisizione diretta dei dati di traffico telefonico relativi al proprio assistito: limiti normativi e prospettive "de iure condendo"*, in *Arch. nuova proc. pen.*, 1, 2018, p. 1 ss.;
- E. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Milano, 2018;
- E. ANDOLINA, *La raccolta dei dati relativi alla localizzazione del cellulare ed al traffico telefonico tra inerzia legislativa e supplenza giurisprudenziale*, in *Arch. Pen.*, 3, 2020, p. 1 ss.;
- E. ANODINA, *Cooperazione-integrazione penale nell'Unione Europea*, in *Cass. pen.*, 10, 2001, p. 2898 ss.;
- F. ANTOLISEI, *Manuale di diritto penale*, Milano, 2003;
- A. ANZON, *Interpretazione "corretta" e interpretazione "conforme a Costituzione" del regime delle rogatorie internazionali*, in *Giur. Cost.*, 4, 2002, p. 2426 ss.;
- E. APRILE, *La tutela dei diritti fondamentali e le nuove garanzie del processo penale*, in AA.VV., *Cooperazione giudiziaria penale nell'Unione europea prima e dopo il Trattato di Lisbona*, (a cura di E. APRILE-F. SPIEZIA), Milano, 2009;
- E. APRILE, *Nuovi strumenti e tecniche investigative nell'ambito U.E.: intercettazioni all'estero, operazioni di polizia oltre frontiera, attività sotto copertura e videoconferenze con l'estero*, in *Cass. pen.*, 1, 2009, p. 440B ss.;
- E. APRILE, *Osservazioni a C. Cost. data udienza (21 febbraio 2018), data deposito 27 aprile 2018, n. 92*, in *Cass. pen.*, 7-8, 2018, p. 2450b ss.;

- E. APRILE, L. DANIELE, *Cooperazione giudiziaria penale nell'Unione europea prima e dopo il Trattato di Lisbona*, Milano, 2009;
- E. APRILE, F. SPIEZIA, *Cooperazione giudiziaria penale nell'Unione Europea prima e dopo il Trattato di Lisbona*, Milano, 2009;
- G.A. ARIELY, *Adaptive Responses to Cyberterrorism*, in T.M. CHEN, L. JARVIS, S. MACDONALD (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, 2014;
- M. ARLEO, *Commento a Corte cost.*, 8 novembre 2007 – 21 febbraio 2018, n. 33, in AA.VV., *Corte costituzionale e sistema processuale penale. L'elaborazione giurisprudenziale del 2018* (a cura di D. CIMADOMO, G. DALIA), Milano, 2019, p. 1 ss.;
- I. ARMADA, *The European Investigation Order and the lack of European Standards for Gathering Evidence: Is a fundamental Rights-based Refusal the solution?*, in *New Journal of European Criminal Law*, 1, 2015;
- I. ARMADA, A. WEYEMBERGH, *The mutual recognition principle and EU Criminal law*, in AA.VV., *The European Union as an Area of Freedom, Security and Justice* (a cura di M. FLETCHER, E. HERLIN-KARNELL, C. MATERA), London, 2017;
- A. ARNULL, *The Principle of Effective Protection in EU Law: An Unruly Horse?*, in *European Law Review*, 1, 2011, p. 51 ss.;
- C. ASARO, *Sul cammina tracciato da Evidence*, in *Inf. e dir.*, 2, 2016, p. 141;
- M. ASCOLI, *La interpretazione delle leggi*, Roma, 1928;
- P. ASP, *Nordic Judicial Co-operation in Criminal Matters*, Uppsala, 1998;
- A. ASTARITA, *Vecchio e nuovo in tema di rogatorie internazionali*, in *Giur. it.*, 1, 2003, p. 150 ss.;
- S. ATERNO, *Profili penali dell'anonimato in rete*, in AA.VV., *Sicurezza e anonimato in rete* (a cura di A. MAGGIPINTI, M. IASELLI), Milano, 2005;
- S. ATERNO, *Acquisizione e analisi della prova informatica*, in *Dir. pen. e proc.*, *Dossier Processo penale e prova scientifica* (a cura di P. TONINI), 6, 2008, p. 61 ss.;
- S. ATERNO, sub art. 8, in AA.VV., *Cybercrime, responsabilità degli enti, prova digitale* (a cura di G. CORASANITI, G. CORRIAS LUCENTE), Padova, 2009;
- S. ATERNO, voce *Digital forensics (investigazioni informatiche)*, in *Dig. disc. pen.*, Agg. VIII, Torino, 2014, p. 217 ss.;
- S. ATERNO, *OSSERVAZIONI a Cass. Pen.*, 27 maggio 2013, n. 40303, sez. I, in *Cass. pen.*, 5, 2014, p. 1706;
- S. ATERNO, *L'acquisizione dei dati personali tra misure antiterrorismo e intromissioni nella privacy*, in *Arch. pen.*, 1, 2016, p. 165 ss.;
- S. ATERNO, *Cloud forensics: aspetti giuridici e tecnici*, in A.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- S. ATERNO, *La Convenzione di Budapest del 2001 e la l. n. 48/2008*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- S. ATERNO, M. MATTIUCI, *Cloud Forensic e nuove frontiere delle indagini informatiche nel processo penale*, in *Arch. pen.*, 3, 2013, p. 865 ss.;
- S. AVVEDUTO, D. LUZI, L. PISACANE, *La categorizzazione del progetto Evidence: la rappresentazione concettuale del dominio "prova elettronica"*, in *Informatica e diritto*, 1-2, 2015, p. 182 ss.;
- L. AYALA, *Cybersecurity Lexicon*, New York, 2016;

- E. AZANI, N. LIV, *A Comprehensive Doctrine for an Evolving Threat: Countering Terrorist Use of Social Networks*, in *Studies in Conflict & Terrorism*, 8, 2020, p. 728 ss.;
- C. BAARTMANS, M. COX, *De nasleep van Schrems II houdt niet over: de gevolgen van de uitspraak van het HvJ EU in Schrems II en de daaropvolgende (concept) aanbevelingen van de EDPD onder de loep genomen*, in *Mediaforum: Tijdschrift voor Media- en Communicatierecht*, 1, 2021, p. 1 ss.;
- G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- G.M. BACCARI, C. CONTI, *La corsa tecnologica tra Costituzione, codice di rito e norme sulla privacy: uno sguardo d'insieme*, in *Dir. pen. proc.*, 6, 2021, p. 711 ss.;
- L. BACHMAIER WINTER, *The Role of the Proportionality Principle in Cross-Border Investigations Involving Fundamental Rights*, in AA.VV., *Transnational Inquiries ad the Protection of Fundamental Rights in Criminal Proceedings. A Study in Memory of Vittorio Grevi and Giovanni Tranchina* (a cura di S. RUGGERI), Berlino, 2013;
- L. BACHMAIER WINTER, *Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la orden europea de investigación*, in *Revista General de Derecho europeo*, 36, 2015, p. 15 ss.;
- L. BACHMAIER WINTER, *Transnational evidence: towards the transposition of Directive 2014/41 regarding the European Investigation Order in criminal matters*, in *Eucrim: the European Criminal Law Associations' forum*, 2, 2015, p. 47 ss.;
- E. BALAJANOV, *Setting the minimum age of criminal responsibility for cybercrime*, in *International Review of Law, Computers & Technology*, 1, 2018, p. 2 ss.;
- V. BALBUZANOVA, *Don't Kill the Messenger How the New Technologies Used by Internet-Based Communications Providers are Gutting Compelled Disclosure Laws*, in *Journal of Law & Cyber Warfare*, 1, 2020, p. 139 ss.;
- A. BALSAMO, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in *Cass. pen.*, 11, 2016, p. 4236 ss.;
- I. BANTEKAS, *The principle of mutual recognition in EU Criminal law*, in *European Law Review*, 3, 2007, p. 365 ss.;
- R. BARATTA, *L'equivalenza delle normative nazionali ai sensi dell'art. 100B del Trattato CE*, in *Rivista di diritto europeo*, 1993, p. 727 ss.;
- A. BARBASCHOW, *New Bill to Prepare Australian Law Enforcement for the US CLOUD Act*, in *ZDNet.com*, 5 marzo 2020;
- E. BARBE, *La coopération judiciaire en matière pénale au sein de l'Union Européenne: les voies incertaines de la reconnaissance mutuelle*, in AA.VV., *La protection des intérêts financiers de l'Union et le rôle de l'Olaf vis-à-vis de la responsabilité pénale des personnes morales et des chefs d'entreprises et admissibilité mutuelle des preuves (Acts des Journées d'études de Inverigo – Como)* (a cura di F. RUGGERI), Bruylant, Bruxelles, 2005;
- E. BARBE, G. RENAUDINEAU, *L'espace de liberté, de sécurité et de justice*, in J. ZILLER, *L'Union européenne: édition traité de Lisbonne*, Paris, 2008;
- A. BARBERA, *La Carta dei diritti: per un dialogo fra la Corte italiana e la Corte di giustizia*, in *Quaderni Costituzionali*, 2018, 1, p. 149 ss.;

- A. BARBIERI, *Le attività d'indagine della polizia giudiziaria su sistemi informatici e telematici (commento a l. 18 marzo 2008, n. 48)*, in *Diritto dell'internet*, 5, 2008, p. 516 ss.;
- U. BARDARI, *Le identità nei social network: strumenti tecnici virtuali con conseguenze giuridiche reali*, in AA.VV., *Questioni di informatica forense* (a cura di C. MAIOLI), Roma, 2015;
- A. BARGI, *Intercettazioni telefoniche: effettività della difesa e imprevedibilità delle decisioni di legittimità*, in *Giur. It.*, 3, 2011, p. 729 ss.;
- A. BARGI, *Le prove e le decisioni*, in AA.VV., *Procedura penale* (a cura di A. GAITO), Milano, 2018;
- M. BARGIS, *La cooperazione giudiziaria penale nell'Unione europea tra mutuo riconoscimento e armonizzazione: analisi e prospettive*, in *Riv. Dir. Proc.*, 4, 2012, p. 914 ss.;
- M. BARGIS, *L'attuazione della direttiva (UE) 2016/1919 nei procedimenti di esecuzione del mandato di arresto europeo fra scelte positive e lacune strutturali*, in *Sistema penale*, 11, 2019, p. 85 ss.;
- B. BARNETT, J.A. BROWN, O. FASSHAUER, V.L. FRANCIS, T.E. YALE, *Forecasting the Impact of the New US CLOUD Act*, Filadelfia, 2018;
- R.M.F. BARON, *A Critique of the International Cybercrime Treaty*, in *CommLaw Conspectus*, 2, 2002, p. 263 ss.;
- G. BARROCU, *Rogatorie penali internazionali*, in *Enc. dir.*, XXX, Roma, 2008;
- G. BARROCU, *La cooperazione investigativa in ambito europeo. Da Eurojust all'ordine di indagine*, Milano, 2017;
- G. BARROCU, *Le speciali tecniche di investigazione nel contesto europeo*, in *Cass. pen.*, 3, 2020, p. 1325 ss.;
- L. BARTOLI, *Sequestro dei dati a fini probatori: soluzioni provvisorie a incomprensioni durature*, in *Arch. Pen. online*, 1, 2018, p. 1 ss.;
- V.L. BARTOLI, *Digital evidence for the criminal trial: limitless cloud and state boundaries*, in *Big data and Public Law: new challenges beyond data protection*, in *rivista.eurojus.it*, num. spec., 2019, p. 102 ss.;
- L. BARTOLI, C. MAIOLI, *La catena di custodia del dato digitale: tra anelli solidi e anelli mancanti*, in *Informatica e diritto*, 1-2, 2015, p. 139 ss.;
- F. BASILE, *Intelligenza artificiale e diritto penale. Quattro possibili percorsi di indagine*, in *Diritto penale e uomo*, 19 settembre 2019;
- F. BASSANINI, E. BELLONI, *L'impatto del cloud computing sull'economia italiana*, Roma, 2011;
- G. BATTARINO, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021, n. 132*, in *Questione giustizia*, 5 ottobre 2021;
- Z. BAUMAN, *Dentro la globalizzazione. Le conseguenze sulle persone*, Roma-Bari, 1998;
- P. BEAUVAIS, M. BENLOLO-CARABOT, *Droit pénal de l'Union européenne*, in *Revue trimestrielle de droit européen*, 4, 2017, p. 884 ss.;
- R. BELFIORE, *Il mandato europeo di ricerca delle prove e l'assistenza giudiziaria nell'Unione europea*, in *Cass. pen.*, 10, 2008, p. 3894 ss.;

- R. BELFIORE, *Movement of Evidence in the EU: The Present Scenario and Possible Future Developments*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 17, 2009, p. 1 ss.;
- R. BELFIORE, *La prova penale "raccolta" all'estero*, Roma, 2014;
- R. BELFIORE, *Riflessioni a margine della direttiva sull'Ordine europeo di indagine penale*, in *Cass. Pen.*, 9, 2015, p. 3288C ss.;
- R. BELFIORE, *Su alcuni aspetti del decreto di attuazione dell'ordine europeo di indagine penale*, in *Cass. Pen.*, 1, 2018, p. 400 ss.;
- M. BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle Sezioni Unite*, in *penalecontemporaneo.it*, 2 febbraio 2015;
- G. BELLAVISTA, *Lezioni di diritto processuale penale* (a cura di G. TRANCHINA), Milano, 1979;
- T. BENE, *Transnazionalità dei crimini e la società confessionale: i pericoli della tecnologia e del diritto*, in *Giur. It.*, 3, 2016, p. 717 ss.;
- T. BENE, L. LUPARIA, L. MARAFIOTI (a cura di), *L'ordine europeo di indagine. Criticità e prospettive*, Torino, 2016;
- J. BENIGER, *The control revolution. Technological and economic origins of the information society*, Harvard, 1986;
- S.W. BENNER, *Defining Cybercrime: a Review of Federal and State Law*, in R.D. CLIFFORD (ed.), *Cybercrime: The Investigation, Prosecution, and Defense of a Computer-Related Crime*, 3rd ed., Raleigh, 2011;
- G. BENTHAM, *Teoria delle prove giudiziarie*, Bruxelles, 1842;
- V. BERLINGÒ, *Il fenomeno della datafication e la sua giuridicizzazione*, in *Riv. trim. dir. pubbl.*, 3, 2017;
- A. BERNARDI, *Strategie per l'armonizzazione dei sistemi penali europei*, in AA.VV., *Il diritto penale nella prospettiva europea* (a cura di S. CANESTRARI, L. FOFFANI), Milano, 2005;
- A. BERNARDI, *La competenza penale accessoria dell'Unione europea: problemi e prospettive*, in *Dir. pen. cont.*, 1, 2012, p. 43 ss.;
- A. BERNARDI, D. NEGRI, *Rapporti tra autorità giudiziarie nazionali e organi investigativi nell'ottica della futura istituzione della Procura europea: modelli operazionali e buone pratiche nella lotta ai reati che ledono gli interessi finanziari dell'UE*, in *penalecontemporaneo.it*, 10 febbraio 2015;
- A. BERNASCONI, *Sistema probatorio e disposizioni generali*, in AA.VV., *Manuale di diritto processuale penale*, Torino, 2015;
- V. BERRA, *Armi, droga e malware. Tutto quello che potevate trovare nel "Berlusconi Market", il negozio "più affidabile" del dark web*, in *Open.online*, 7 novembre 2019;
- R. BERTUOL, *La nuova disciplina per l'acquisizione dei tabulati telefonici: l'interpretazione "autentica" del Legislatore e la parola fine alla (fin troppo) lunga querelle giurisprudenziale*, in *Giurisprudenza Penale Web*, 12, 2021, p. 1 ss.;
- J. BESSANT, *Human Rights, the Law, Cyber-security and Democracy: After the European Convention*, in *Australian Journal of Human Rights*, 1, 2012, p. 1 ss.;
- G. BETTIOL, L. PETTOELLO MANTOVANI, *Diritto penale*, Padova, 1986;

- M.A. BIASIOTTI, *Presente e futuro dello scambio della prova elettronica in Europa*, in *Informatica & diritto*, 1-2, 2015, p. 50 ss.;
- M.A. BIASIOTTI, S. CONTI, F. TURCHI, *La raccolta transnazionale della prova digitale in ambito europeo: una proposta per l'adozione di uno standard*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- P. BIDDLE, P. ENGLAND, M. PEINADO, B. WILLMAN, *The Darknet and the Future of Content Protection*, in AA.VV., *Digital Rights Management* (a cura di J. FEIGENBAUM), Berlino, 2003;
- A. BIGIARINI, *Mandato di arresto europeo e reciproco riconoscimento delle sentenze penali nei processi in absentia*, in *Dir. pen. e proc.*, 8/9, 2016, p. 999 ss.;
- P. BILANCIA, *Lo spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria*, in *Riv. It. Dir. pubbl. comunit.*, 2, 2004, p. 349 ss.;
- P. BILANCIA, *Lo spazio di libertà, sicurezza e giustizia tra realtà intergovernativa e prospettiva comunitaria*, in AA.VV., *Alle frontiere del diritto costituzionale: scritti in onore Valerio Onida* (a cura di M. D'AMICO, B. RANDAZZO), Milano, 2011;
- S. BILGIC, *Something Old, Something New, And Something Moot: The Privacy Crisis Under the CLOUD Act*, in *Harvard Journal of Law & Technology*, 1, 2018, p. 321 ss.;
- C. BILLET, *Une nouvelle revendication de l'autonomie de l'ordre juridique de l'Union européenne: (CJUE, avis 1/15 du 26 juillet 2017, projet d'accord entre le Canada et l'Union européenne sur le transfert et le traitement des données des dossiers passagers)*, in AA.VV., *Annuaire français de droit international*, LXIII/2017, Parigi, 2018;
- G. BIONDI, *La giurisprudenza in tema di investigazioni difensive, con particolare riferimento all'attività di assunzione di informazioni*, in *Giur. Merito*, 4, 2008, p. 923B ss.;
- R. BISMUTH, *Le Cloud Act face au project européenne e-evidence: confrontation ou coopération?*, in *Revue de droit international privé*, 3, 2019, p. 685 ss.;
- G. BISOGNI, G. BRONZINI, V. PICCONE (a cura di), *La Carta dei diritti dell'Unione europea. Casi e materiali*, Taranto, 2009;
- J. BLACKSTOCK, *The European Investigation Order*, in *New Journal of European Criminal Law*, 4, 2010, p. 481 ss.;
- B.J. BLAŽIČ, T. KLOBUČAR, *Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society*, in *Information & Communication Technology Law*, 1, 2020, p. 66 ss.;
- M. BOLOGNARI, *Ordine europeo di indagine penale ed esame a distanza*, in *Riv. dir. proc.*, 4-5, 2018, p. 1100 ss.;
- S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Democrazia e Sicurezza*, 3, 2014, p. 1 ss.;
- M. BORDIERI, *Brevi note sull'inutilizzabilità di atti di investigazione svolti all'estero dal difensore dell'imputato senza passare attraverso una rogatoria internazionale*, in *Cass. pen.*, 5, 2009, p. 2035 ss.;
- M.J. BORGERS, *Functions and aims of harmonisation after the Lisbon Treaty: a European Perspective*, in AA.VV., *The future of police and judicial cooperation in the European Union* (C. FIJNAUT, J. OUWERKERK eds.), Leiden, 2010;
- M. BORRACCETTI, *Art. 47*, in AA.VV., *La Carta dei diritti dell'Unione europea. Casi e materiali* (a cura di G. BISOGNI, G. BRONZINI, V. PICCONE), Taranto, 2009;

- R. BORRUSO, S. RUSSO, C. TIBERI, *L'informatica per il giurista*, Milano, 2009;
- M. BÖSE, *La sentenza della Corte costituzionale tedesca sul Trattato di Lisbona e il suo significato per la europeizzazione del diritto penale*, in *Criminalia*, 2009, p. 267 ss.;
- F. BRICOLA, *Il costo del principio "societas delinquere non potest" nell'attuale dimensione del fenomeno societario*, in *Riv. it. dir. e proc. pen.*, 1970, p. 951 ss.;
- C. BRIÈRE, *La jurisprudence de la Cour de justice et du Tribunal de l'Union européenne. Chronique des arrêts. Arrêt «Radu»*, in *Revue du droit de l'Union européenne*, 1, 2013, p. 171 ss.;
- C. BRIÈRE, *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, in *European Papers*, 1, 2021, p. 493 ss.;
- F. BUFFA, *Internet e criminalità. Finanza telematica off shore*, Milano, 2011;
- T. BUNYAN, *Trevi, Europol and European state*, in *Statewhaching the new europe*, 1993, p. 1 ss.;
- L. BUONO, *The genesis of European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, in *ERA Forum*, 19, 2019, p. 308 ss.;
- L. BUONO, *The genesis of the European Union's new proposed legal instrument(s) on e-evidence. Towards the EU Production and Preservation Orders*, in *ERA Forum*, 3, 2019, p. 307 ss.;
- F. BUONOMENNA, *Profili evolutivi di sussidiarietà europea e di sovranità inclusiva*, in *Rivista della cooperazione giuridica internazionale*, 56, 2017, p. 153 ss.;
- N. BURLEIGH, *The Rise and Fall of Silk Road, the Dark Web's Amazon*, in *Newsweek*, 19 febbraio 2015;
- A. CABIALE, *Pubblicata la direttiva 2014/41/UE sull'ordine europeo d'indagine penale: semplificazioni, (s)fiducia reciproca e compromessi, per tentare di superare le rogatorie*, in *Proc. pen. e giust.*, 5, 2014, p. 15 ss.;
- A. CABIALE, *I limiti alla prova nella procedura penale europea*, Milano, 2019;
- D. CACCAVELLA, *Informatica forense e linea del tempo*, Relazione presentata al convegno "Nuove prospettive sui reati informatici", Venezia, 27 maggio 2006, paper;
- R. CAFARI PANICO, *Lo spazio di libertà, sicurezza e giustizia nel Trattato di riforma e nel Trattato costituzionale*, in AA.VV., *Dalla Costituzione europea al Trattato di Lisbona* (a cura di M.C. BARUFFI) Padova, 2008;
- G. CAGGIANO, *L'evoluzione dello spazio di libertà, sicurezza e giustizia nella prospettiva di un'Unione basata sul diritto*, in *Studi sull'integrazione europea*, 2, 2007, p. 335 ss.;
- M. CAGOSI, *Un illustre assente: la vittima del reato nell'ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016;
- M. CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. pen. cont.*, 3-4, 2014, p. 145 ss.;
- M. CAIANIELLO, *Dal Terzo pilastro ai nuovi strumenti: diritti fondamentali, "road map" e l'impatto delle nuove direttive*, in AA.VV., *I nuovi orizzonti della giustizia penale europea*, Atti del convegno ASPP, Milano, 24-26 ottobre 2014, Milano, 2015;

- M. CAIANIELLO, *La nuova direttiva UE sull'ordine europeo di indagine penale tra mutuo riconoscimento e ammissione reciproca delle prove*, in *Proc. pen. e giust.*, 3, 2015, p. 1 ss.;
- M. CAIANIELLO, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in *Cass. Pen.*, 6, 2018, p. 2197 ss.;
- M. CAIANIELLO, *L'OEI dalla direttiva al decreto n. 108 del 2017*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- A. CAIOLA, *Retour sur la mise en œuvre du mandat d'arrêt européen: le respect de l'interdiction des traitements inhumains ou dégradants dans la détention*. CJUE, gde ch., 15 octobre 2019, Dumitru-Tudor Dorobantu/Hanseatisches Oberlandesgericht Hamburg, C-128/18, ECLI:EU:C:2019:857, in *Revue des affaires européennes*, 4, 2019, p. 785 ss.;
- F. CAJANI, *Interception of communications: Skype, Google, Yahoo! And Microsoft tools and electronic data retention on foreign servers: A legal perspective from a prosecutor conducting an investigation*, in *Digital Evidence and Electronic Signature Law Review*, 6, 2009, p. 158 ss.;
- F. CAJANI, *La Convenzione di Budapest nell'insostenibile salto all'indietro del Legislatore italiano, ovvero: quello che le norme non dicono...*, in *Cyberspazio e diritto*, 1, 2010, p. 185 ss.;
- F. CAJANI, *Le indagini informatiche per i reati di cyberterrorismo*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- O. CALAVITA, *La proposta di Regolamento sugli ordini di produzione e conservazione europei: Commissione, Consiglio e Parlamento a confronto*, in *Leg. Pen.*, 30 marzo 2021;
- O. CALAVITA, *Ordine europeo di indagine e rimedi interni: riflessioni sulle prime applicazioni giurisprudenziali*, in *Leg. Pen.*, 30 settembre 2021;
- P. CALAMANDREI, *Il processo come giuoco*, Milano, 1950;
- E. CALVANESE, *Cooperazione giudiziaria tra Stati e trasmissione spontanea di informazioni: condizioni e limiti di utilizzabilità*, in *Cass. pen.*, 2, 2003, p. 458 ss.;
- E. CALVANESE, G. DE AMICIS, *Appunti sulla Nuova Convenzione di assistenza giudiziaria penale tra gli Stati membri dell'Unione europea*, in *Giur. Merito*, 4-5, 2000, p. 1052 ss.;
- L. CAMALDO (a cura di), *L'istituzione del Procuratore europeo e la tutela penale degli interessi finanziari dell'Unione europea*, Torino, 2014;
- L. CAMALDO, *La direttiva sull'ordine europeo di indagine penale (OEI): un congegno di acquisizione della prova dotato di molteplici potenzialità, ma di non facile attuazione*, in *penalecontemporaneo.it*, 27 maggio 2014, p. 1 ss.;
- L. CAMALDO, *La nuova fisionomia della procura europea all'esito del semestre di presidenza italiana del Consiglio europeo*, in *Cass. pen.*, 2, 2015, p. 0804B ss.;
- L. CAMALDO, *La normativa di attuazione dell'ordine europeo di indagine penale: le modalità operative del nuovo strumento di acquisizione della prova all'estero*, in *Cass. Pen.*, 11, 2017, p. 4196B ss.;
- L. CAMALDO, *L'istituzione della Procura europea: il nuovo organo investigativo affonda le proprie radici negli ordinamenti nazionali*, in *Cass. pen.*, 2018, p. 958 ss.;

- L. CAMALDO, F. CERQUA, *La direttiva sull'ordine europeo di indagine penale: le nuove prospettive per la libera circolazione delle prove*, in *Cass. Pen.*, 10, p. 3511 ss.;
- L. CAMALDO, F. MANFREDINI, *La cooperazione giudiziaria nell'era delle minacce globali e la riforma del libro XI del codice di procedura penale*, in *Cass. Pen.*, 7/8, 2016, p. 3043B ss.;
- I. CAMINITI, *L'effettiva portata del principio locus regit actum*, in *Giur. It.*, 10, 2002, p.1919 ss.;
- A. CAMON, *The project devices and digital evidence in Europe*, in M. CAIANIELLO, A. CAMON, *Digital Forensic Evidence. Towards Common European Standards in Antifraud Administrative and Criminal Investigations*, Milano, 2021;
- S. CAMPAILLA, *La "circolazione" giudiziaria europea dopo Lisbona*, in *Proc. pen. e giust.*, 5, 2011, p. 90 ss.;
- V. CAMPILONGO, *L'obbligo di motivazione in tema di intercettazioni di conversazioni o comunicazioni: questioni interpretative e problemi applicativi*, in *Cass. pen.*, 10, 2005, p. 3196 ss.;
- D. CANGEMI, *Procedural Law Provisions of the Council of Europe Convention on cybercrime*, in *International Review of Law, Computers & Technology*, 2, 2004, p. 165 ss.;
- E. CANNIZZARO, *La riparazione dei danni da attività giudiziaria nel diritto dell'Unione europea*, in AA.VV., *La vittima del processo. I danni da attività processuale penale* (a cura di G. SPANGHER), Torino, 2017;
- E. CANNIZZARO, *La cornice europea*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale*, Salerno, 25-27 ottobre 2018 (a cura di L. KALB), Milano, 2019;
- G. CANSACCHI, *Assistenza giudiziaria internazionale*, in *Novissimo Digesto Italiano*, vol. I, Torino, 1964;
- G. CANZIO, *Prova scientifica, ricerca della «verità» e decisione giudiziaria nel processo penale*, in *Decisione giudiziaria e verità scientifica*, Quaderni della Rivista trimestrale di diritto e procedura civile, 3, 2005, p. 55 ss.;
- F. CAPOTORTI, *Il diritto dei trattati secondo la Convenzione di Vienna*, in *Convenzione di Vienna sul diritto dei trattati*, Padova, 1969;
- F. CAPRIOLI, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista Brasileira de direito Processual Penal*, 2, 2017, p. 483 ss.;
- P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Arch. pen.*, 1, 2016, p. 28 ss.;
- I. CARACCILO, *Dal diritto penale internazionale al diritto internazionale penale*, Napoli, 2000;
- D. CARCANO, *In tema di rogatorie internazionali*, in *Cass. pen.*, 11, 2002, p. 3333 ss.;
- D. CARCANO, *Principi generali della disciplina*, in AA.VV., *Rogatorie penali e cooperazione giudiziaria internazionale* (a cura di E. CALVARESE, G. LA GRECA, M.R. MARCHETTI), Torino, 2003;
- D. CARDAMONE, *La sentenza della Cedu Brazzi c. Italia: sono arbitrarie le perquisizioni disposte dall'Autorità giudiziaria?*, in *Questione Giustizia*, 15 gennaio 2019, p. 1 ss.;

- M. CERESA GASTALDO, *La responsabilità degli enti: profili di diritto processuale*, in AA.VV., *Impresa e giustizia penale: tra passato e futuro*. Atti del Convegno. Milano, 14-15 marzo 2008, Milano, 2009;
- P. CARETTI, *I diritti fondamentali. Libertà e Diritti sociali*, II ed., Torino, 2005;
- P. CARETTI, A. CARDONE, *Diritto dell'informazione e della comunicazione nell'era della convergenza. Stampa, radiotelevisione, telecomunicazioni, internet, teatro e cinema*, Bologna, 2019;
- L. CARLASSARE, *Regolamenti dell'esecutivo e principio di legalità*, Padova, 1966;
- F. CARNELUTTI, *Lezioni sul processo penale*, Roma, 1947, p. 210; ID., *Diritto e processo*, Napoli, 1958;
- S. CARRERA, G.G. FUSTER, E. GUILD, V. MITSILEGAS, *Access to Electronic Data by Third-Country Law Enforcement Authorities. Challenges to EU Rule of Law and Fundamental Rights*, in *Centre for European Policy Studies*, 8 luglio 2015;
- S. CARRERA, M. STEFAN, *Access to Electronic Data for Criminal Investigations Purposes in the EU*, in *CEPS Paper*, Brussels, 2020;
- M. CARTABIA, *Edipo Re*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), Bologna, 2018;
- M. CARTABIA, *L'impatto costituzionale della Carta dei Diritti dell'Unione europea*, in AA.VV., *Liber Amicorum Antonio Tizzano*, Torino, 2018;
- M. CARTABIA, L. VIOLANTE, *Conflitti tragici, conflitti giuridici*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), Bologna, 2018;
- M. CARTABIA, L. VIOLANTE, *Le leggi cambiano, la loro interpretazione evolve*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), Bologna, 2018;
- M. CARTABIA, L. VIOLANTE, *Teatro e processo penale*, in AA.VV., *Giustizia e mito* (a cura di M. CARTABIA, L. VIOLANTE), Bologna, 2018;
- C.M. CASCIONE, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione data retention della Corte di giustizia e gli echi del datagate*, in *Nuova giur. civ. comm.*, 11, 2014, p. 1044 ss.;
- E. CASEY, *Digital evidence and computer crime. Forensic science, computers and the internet*, London-San Diego, 2000;
- E. CASEY, *Digital Evidence and Computer Crime. Forensic Science, Computers, and the Internet*, Amsterdam, 2011;
- G. CASELLI, G. DE AMICIS, *La natura di Eurojust e la sua attuazione nell'ordinamento interno*, in *Dir. e giustizia*, 2003, p. 94 ss.;
- A. CASSESE, *The Multifaceted Criminal Notion of Terrorism in International Law*, in *Journal of International Criminal Justice*, 5, 2006, p. 933 ss.;
- M. CASTELLS, *The age of information*, Oxford, 1996;
- M. CASTELLS, *La nascita della società in rete*, Milano, 2014;
- E.M. CATALANO, *L'abuso del processo*, Milano, 2004;
- G. CATELANI, *I rapporti internazionali in materia penale*, Milano, 1995;
- S. CENTONZE, L. GIOVEDÌ, *La direttiva antiterrorismo 2017/541 del 15 marzo 2017*, in *Il Penalista*, 31 maggio 2017;
- F. CENTORAME, *Le indagini tecnologiche ad alto potenziale intrusivo fra esigenze di accertamento e sacrale inviolabilità dei diritti della persona*, in *Riv. it. dir. e proc. pen.*, 2021, p. 502;

- C. CESARI, *L'impatto delle nuove tecnologie sulla giustizia penale – un orizzonte denso di incognite*, in *Rev. Bras. de Direito Processual Penal*, 3, 2019, p. 1167 ss.;
- E. CESQUI, *Il ruolo del Ministero nella cooperazione penale*, in *Cass. pen.*, 1, 2019, p. 14 ss.;
- M. CHAVES, *EU's Harmonization of National Criminal Law: Between Punitiveness and Moderation*, in *European public law*, 3, 2015, p. 57 ss.;
- R. CHENAL, *Il diritto al rispetto del domicilio in caso di perquisizione (art. 8 CEDU)*, in AA.VV., *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno (2016-2020)* (a cura di A. DI STASI), Milano, 2020;
- C. CHEVALLIER-GOVERS, *Le traité de Lisbonne et la différenciation dans l'espace de liberté, de sécurité et de justice*, in E. BROSSET, C. CHEVALLIER-GOVERS, V. EDJAHARIAN, *Le traité de Lisbonne: déconstitutionnalisation ou reconfiguration de l'Union européenne?*, Bruxelles, 2009;
- C. CHEVALLIER-GOVERS, *L'Espace de liberté, de sécurité et de justice (ESLJ)*, in *Revue du droit de l'Union Européenne*, 2, 2018, p. 114 ss.;
- A. CHIARI, *La prova digitale: le sentenze sulla rilevanza probatoria e l'acquisizione*, in *Quot. Giur.*, 26 luglio 2018;
- M. CHIAVARIO, *Cooperazione internazionale ed obiettivi di garanzia e di efficienza nella nuova disciplina dei rapporti con autorità giudiziarie straniere*, in *Leg. Pen.*, 4, 1990, p. 687 ss.;
- M. CHIAVARIO, sub *Art. 275 c.p.p.*, in AA.VV., *Commento al nuovo codice di procedura penale* (a cura di M. CHIAVARIO), Torino, 1990;
- M. CHIAVARIO, *Cooperazione giudiziaria e di polizia in materia penale a livello europeo*, in *Riv. It. Dir. Proc. Pen.*, 3, 2005, p. 974 ss.;
- M. CHIAVARIO, *Giustizia europea e processo penale: nuovi scenari e nuovi problemi*, in *Leg. pen.*, 2008, p. 468 ss.;
- M. CHIAVARIO, *Giustizia europea e processo penale: nuovi scenari e nuovi problemi*, in AA.VV., *Processo penale e giustizia europea. Omaggio a Giovanni Conso* (a cura di U. DRAETTA, N. PARISI), Milano, 2010;
- M. CHIAVARIO, *Diritto processuale penale*, Torino, 2015;
- T. CHRISTAKIS, *21 Thoughts and Questions about the UK-US CLOUD Act Agreement: (and an Explanation of How it Works – with Charts)*, in *European Law Blog*, 13 ottobre 2019, p. 1 ss.;
- T. CHRISTAKIS, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities After the CLOUD Act: Is There a Conflict with the GDPR?*, in AA.VV., *Cybersecurity and Privacy in a Globalized World – Building Common Approches* (P. MILCH, S. BENTHALL eds.), New York, 2019;
- H. CHRISTODOULOU, L. GAURIER, A. MORNET, *La proposition e-evidence: révélatrice des limites de l'émergence d'une procédure pénale européenne ou compromis nécessaire?*, in *European Papers*, 1, 2021, p. 423 ss.;
- A. CIAMPI, *L'assunzione di prove all'estero in materia penale*, Milano, 2003;
- D. CIMADOMO, *Ordine europeo di indagine penale e garanzie della difesa. Brevi osservazioni a margine della direttiva 2014/41/UE*, in AA.VV., *L'ordine europeo di*

- indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016, p. 219 ss.;
- D. CIMADOMO, *Prova e giudizio di fatto nel processo penale a carico degli enti*, Milano, 2016;
- D. CIMADOMO, *Reciproco riconoscimento e “misure alternative” alla detenzione cautelare*, in AA.VV., *Cooperazione giudiziaria: le novità del recepimento delle fonti sovranazionali. Estratto* (a cura di L. KALB), in *Dir. pen. e proc.*, 8/9, 2016, p. 1015 ss.;
- D. CIMADOMO, *La difesa dell’ente sottoposto a procedimento penale*, in *Proc. pen. e giust.*, 5, 2017, p. 942 ss.
- D. CIMADOMO, *Commento agli artt. 1-9 d. legisl. 7 agosto 2015, n. 137 (Attuazione della decisione quadro 2006/783/GAI relativa all’applicazione del principio del reciproco riconoscimento delle decisioni di confisca)*, in AA.VV., *Commentario breve al Codice antimafia e alle altre procedure di prevenzione* (a cura di G. SPANGHER, A. MARANDOLA), Milano, 2019;
- D. CIMADOMO, *Le modifiche in tema di responsabilità “amministrativa” degli enti derivante da reato*, in AA.VV., *La nuova disciplina dei delitti di corruzione. Profili penali e processuali (L. 9 gennaio 2019, n. 3 c.d. “spazzacorrotti)* (a cura di G. FLORA, A. MARANDOLA), Pisa, 2019;
- D. CIMADOMO, *La sospensione dei termini di durata delle misure cautelari personali per emergenza epidemiologica da Covid-19. A proposito di virus...*, in *Dir. pen. e proc.*, 7, 2020, p. 915 ss.;
- D. CIMADOMO, *Brevi considerazioni in tema di simultaneous processus nel “sistema 231”*, in *Riv. Pen.*, 11, 2021, p. 1012 ss.;
- P. CIRILLO, *Il volto dei reati di opinione nel contrasto al terrorismo internazionale al tempo di Internet*, in *Dir. pen. cont.*, 2, 2019, p. 81 ss.;
- A. CISTERNA, *Un passo importante per omologare le investigazioni Ue*, in *Guida al diritto*, 40, 2017, p. 39 ss.;
- S. CIVATARESE MATTEUCCI, F. GUARRIELLO, P. PUOTI, *Diritti fondamentali e politiche dell’Unione europea dopo Lisbona*, Rimini, 2013;
- S. CIVELLO CONIGLIARO, S. LO FORTE, *Cooperazione giudiziaria in materia penale e tutela dei diritti fondamentali nell’Unione Europea*, in *penalecontemporaneo.it*, 3 giugno 2013;
- R.A. CLARKE, M. MORELL, G. STONE, C. SUSTEIN, P. SWIRE, *Liberty and Security in a Changing World: Report and Recommendations of the President’s Review Group on Intelligence and Communications Technologies*, 18 dicembre 2013;
- F. CLEMENTI, *Lo spazio di libertà, sicurezza e giustizia*, in AA.VV., *Le nuove istituzioni europee: commento al Trattato di Lisbona* (a cura di D. RINOLDI), Bologna, 2010;
- J. CLOUGH, *A World of Difference: the Budapest Convention On Cybercrime and the Challenges of Harmonisation*, in *Monash University Law Review*, 3, 2014, p. 698 ss.;
- A. COLAIOCCO, *La rilevanza delle best practices nell’acquisizione della digital evidence alla luce delle novelle sulla cooperazione giudiziaria*, in *Arch. pen.*, 1, 2019, p. 5;
- B. COLLIN, *The Future of Cyberterrorism*, in *Crime and Justice International*, marzo 1997, p. 15 ss.;

- E. COLOMBO, *Ordini europei di produzione e di conservazione delle prove elettroniche in materia penale: il difficile approccio del diritto alla tecnologia nella proposta di regolamento*, in *Cass. pen.*, 7, 2019, p. 2722 ss.;
- K. CORNILS, *Il luogo di commissione dei reati di manifestazione del pensiero in internet*, in *Diritto dell'informazione e dell'informatica*, 4/5, 2002, p. 891 ss.;
- COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS, *Draft report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, 24 ottobre 2019;
- M. CONDINANZI, *Fonti del "terzo pilastro" dell'Unione europea e ruolo della Corte costituzionale*, in *Diritto dell'Unione Europea*, 2007, p. 513 ss.;
- M. CONDINANZI, Sub art. 47, in AA.VV., *Commentario breve ai Trattati dell'Unione europea*, Padova, 2014;
- B. CONFORTI, *Diritto internazionale*, Napoli, 2014;
- CONSIGLIO D'EUROPA, *Guida alla prova digitale*, Strasburgo, 2013;
- G. CONSO, *Il principio della certezza del giudice ed i limiti che lo condizionano*, in AA.VV., *Costituzione e processo penale* (a cura di CONSO), Milano, 1969;
- G. CONSO, *Validità costituzionale della rimessione per motivi d'ordine pubblico o per legittimo sospetto*, in AA.VV., *Costituzione e processo penale* (a cura di G. CONSO), Milano, 1969;
- C. CONTI, *Intercettazioni e inutilizzabilità: la giurisprudenza aspira al sistema*, in *Cass. pen.*, 10, 2011, p. 3638B ss.;
- C. CONTI, *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali*, in *Cass. pen.*, 2, 2013, p. 485 ss.;
- C. CONTI, *L'acquisizione dei tabulati (c.d. data retention)*, in P. TONINI, C. CONTI, *Il diritto delle prove penali*, Milano, 2014;
- C. CONTI, *La prova informatica e il mancato rispetto della best practice: lineamenti sistematici sulle conseguenze processuali*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- C. CONTI, M. TORRE, *Spionaggio digitale nell'ambito dei social network*, in AA.VV., *Le indagini atipiche* (a cura di A. SCALFATI), Torino, 2019;
- I. CONTI, *Il processo penale al tempo del COVID-19: le udienze a distanza*, in *Penale diritto e procedura*, 18 marzo 2020;
- R. CONTI, *Il principio di effettività della tutela giurisdizionale ed il ruolo del giudice: l'interpretazione conforme*, in *Politica del diritto*, 3, 2007, p. 377 ss.;
- S. CONTI, *La legislazione in materia di prove digitali nell'ambito del processo penale. Uno sguardo all'Italia*, in *Informatica & diritto*, 1-2, 2015, p. 153 ss.;
- F. CORDERO, *Connessione e giudice naturale*, in AA.VV., *Connessione di procedimenti e conflitti di competenza* (Atti del Convegno di studio svoltosi a Trieste-Grignano, 3-5 ottobre 1975), Milano, 1976;
- F. CORDERO, *Procedura penale*, Milano, 2012;
- L. CORDÌ, L. 18.3.2008, n. 48 (*Criminalità informatica*) – Art. 8, in *Leg. Pen.*, 2008, p. 286 ss.;
- M. CORHAY, *Private Life, Personal Data Protection and Role of Service Providers: the EU e-Evidence Proposal*, in *European Papers*, 1, 2021, p. 441 ss.;

- O. CORTEN, P. KLEIN, *The Vienna Conventions on the Law of Treaties: a Commentary*, 2 voll., Oxford, 2011;
- G. COSTABILE, *Computer forensics e informatica investigativa alla luce della Legge n. 48 del 2008*, in *Cyberspazio e diritto*, 3, 2010, p. 465 ss.;
- P. COSTANZO, *Aspetti problematici del regime giuspubblicistico di Internet*, in *Problemi dell'informazione*, 2, 1996, p. 183 ss.;
- P. COSTANZO, *Le nuove forme di comunicazione in rete: Internet*, in *Informatica e Diritto*, 1997, p. 25 ss.;
- P. COSTANZO, voce *Internet* (dir. pubbl.), in *Dig. disc. pubbl.*, Agg., Torino, 2000, p. 347 ss.;
- E. COTTU, *Il Consiglio Europeo adotta i nuovi orientamenti strategici per lo spazio di libertà, sicurezza e giustizia per il quinquennio 2015-2020*, in *Diritto Penale Contemporaneo*, 24 luglio 2014;
- COUNCIL OF EUROPE, *Enhanced international cooperation on cybercrime and electronic evidence: towards a protocol to the Budapest Convention*, 14 aprile 2021;
- V. COVOLO, *Mutual Recognition and Absolute Standards of Effective Judicial Protection*, in AA.VV., *Effective Defence Rights in Criminal Proceedings* (a cura di S. ALLEGREZZA, V. COVOLO), Milano, 2018;
- F. CRIMI, *D.L. n. 132/2021: per l'acquisizione dei tabulati telefonici servirà l'autorizzazione del g.i.p.*, in *Quotidiano giuridico*, 5 novembre 2021;
- P. CSONKA, *The Draft Council of Europe Convention on Cyber-Crime: a Response to the Challenge of Crime in the Age of the Internet?*, in *Computer Law & Security Report*, 5, 2000, p. 329 ss.;
- P. CSONKA, *The Council of Europe Convention on Cyber-Crime: a response to the Challenge of the New Age?*, in AA.VV., *Cybercrime: Conferenza internazionale. La Convenzione del Consiglio d'Europa sulla Criminalità Informatica* (a cura di G. ILARDA, G. MARZULLO), Milano, 2004;
- P. CSONKA, A. JUSZCZAK, E. SASON, *The Establishment of the European Public Prosecutor's Office*, in *Eucrim*, 3, 2017, p. 125 ss.;
- L. CUOCOLO, *La qualificazione giuridica dell'accesso a Internet, tra retoriche globali e dimensione sociale*, in *Politica del diritto*, 2/3, 2012, p. 263 ss.;
- D. CURLOTTI, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e "Vecchia Europa": una normativa che non c'è (ancora)*, in *Dir. pen. proc.*, 6, 2021, p. 753 ss.;
- R.J. CURRIE, *Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the "Next Frontier"?*, in *Canadian Yearbook of International Law*, 54, 2017, p. 63 ss.;
- D. CURTOTTI, *Le procedure di consegna della persona: b) il mandato di arresto europeo*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), IV, *Le impugnazioni. Esecuzione penale. Rapporti giurisdizionali con autorità straniere* (a cura di L. KALB), Torino, 2015;
- D. CURTOTTI, *Il captatore informatico nella legislazione italiana*, in *JusOnline*, 3, 2017, p. 382 ss.;
- D. CURTOTTI NAPPI, *I nuovi orizzonti investigativi del difensore: le informazioni assunte all'estero*, in *Giur. It.*, 4, 2008, p. 987 ss.;

- CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #3 – Transborder access to data (Article 32)*, T-CY (2013)7 E, Strasburgo, 3 dicembre 2014;
- CYBERCRIME CONVENTION COMMITTEE (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, T-CY(2016) 5, final report of the T-CY Cloud Evidence Group, Strasburgo, 16 settembre 2016;
- CYBERCRIME CONVENTION COMMITTEE (T-CY), *T-CY Guidance Note #10 – Production orders for subscriber information (Article 18 Budapest Convention)*, T-CY(2015)16, versione rivista adottata dal T-CY a seguito della sedicesima plenaria con procedura scritta il 28 febbraio 2017, Strasburgo, 1 marzo 2017;
- CYBERCRIME CONVENTION COMMITTEE (T-CY), *Guidance Note #11 – Aspects of Terrorism covered by the Budapest Convention*;
- CYBERCRIME CONVENTION COMMITTEE (T-CY), *The Budapest Convention on Cybercrime: benefits and impact in practice*, T-CY (2020)16, Strasburgo, 2020;
- CYBERCRIME PROGRAMME OFFICE OF THE COUNCIL OF EUROPE (C-PROC), *Cooperation between law enforcement and Internet service providers against cybercrime: towards common guidelines*, Bucharest, 2020;
- CYBERCRIME CONVENTION COMMITTEE (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Draft Protocol version 3*, T-CY (2020)7, 28 maggio 2021;
- D. D'AGOSTINI, L. VIOLINO, *Le indagini nei reati informatici*, in AA.VV., *Diritto penale dell'informatica: dai computer crimes alla digital forensic* (a cura di D. D'AGOSTINI), Forlì, 2007;
- M. D'AMICO, *Articolo 47*, in AA.VV., *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea* (a cura di R. BIFULCO, M. CARTABIA, A. CELOTTO), Bologna, 2001;
- F. D'ATH, *Arrêt «Schrems II»: sur la légalité des transferts de données personnelles fondés sur une décision d'adéquation ou moyennant des garanties appropriées*, in *Journal de droit européen*, 10, 2020, p. 442 ss.;
- G. D'AVINO, *Il diritto alla tutela giurisdizionale effettiva nell'art. 47 par. 1 della Carta dei diritti fondamentali dell'UE*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale del Titolo VI della Carta* (a cura di A. DI STASI), Napoli, 2019;
- A. DA FONSECA, *Le Tribunal constitutionnel espagnol et la Cour de justice: un dialogue d'apparat autour de l'affaire Melloni?*, in *gdr-elsj.eu*, 30 marzo 2014;
- G. DA VALLE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 9*, in *Leg. Pen.*, 2008, p. 297 ss.;
- A.A. DALIA, *Sulla precostituzione del giudice naturale come fondamentale garanzia di certezza per l'imputato, con particolare riguardo ai rapporti tra la competenza penale dei consoli e dei comandanti di porto*, in *Riv. it. dir. e proc. pen.*, 1965, p. 507 ss.;
- A.A. DALIA, M. FERRAIOLI, *Manuale di diritto processuale penale*, Padova, 2018;
- G. DALIA, *Il processo contumaciale*, in AA.VV., *«Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012;
- A. DAMATO, P. DE PASQUALE, N. PARISI, *Argomenti di diritto penale europeo*, II ed., Torino, 2014;

- L. DANIELE, *Trattato di Lisbona: addio all'idea federalista per superare gli ostacoli degli euroscettici*, in *Guida. Dir.*, 6, 2007, p. 11 ss.;
- L. DANIELE, *La Carta dei diritti fondamentali dell'Unione europea e il Trattato di Lisbona*, in *Liber Fausto Pocar*, Milano, 2009;
- M. DANIELE, *La prova digitale nel processo penale*, in *Riv. dir. proc.*, 2, 2011, p. 283 ss.;
- M. DANIELE, *Testimony through a Live Link in the Perspective of the Right to Confront Witnesses*, in *Crim. Law Rev.*, 3, 2014, p. 196 ss.;
- M. DANIELE, *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, in *New Journal of European Criminal Law*, 6, 2015, p. 179 ss.;
- M. DANIELE, *La metamorfosi del diritto delle prove nella direttiva sull'ordine europeo di indagine penale*, in *Riv. pen. cont.*, 4, 2015, p. 92 ss.;
- M. DANIELE, *L'impatto dell'ordine europeo di indagine penale sulle regole probatorie nazionali*, in *Dir. Pen. Cont.*, 3, 2016, p. 69 ss.;
- M. DANIELE, *L'ordine europeo di indagine penale*, in *Atti del XXX Convegno Nazionale A.S.P.P. – Investigazioni e prove transnazionali*, Roma, 20-21 ottobre 2016, p. 1 ss.;
- M. DANIELE, *L'ordine europeo di indagine penale entra a regime. Prime riflessioni sul D.Lgs. n. 108 del 2017*, in *Dir. Pen. Cont.*, 7-8, 2017, p. 208 ss.;
- M. DANIELE, *Le indagini informatiche contro il terrorismo. Bilanciamenti difficili e timori legislativi*, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, (a cura di R. WENIN, G. FORNASARI), Napoli, 2017;
- M. DANIELE, *I chiaroscuri dell'OEI e la bussola della proporzionalità*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- M. DANIELE, *La sfera d'uso delle prove raccolte*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- M. DANIELE, *L'acquisizione delle prove digitali dai service provider: un preoccupante cambio di paradigma nella cooperazione internazionale*, in *Rev. Bras. De Direito Processual Penal*, 3, 2019, p. 1280 ss.;
- M. DANIELE, *La collaborazione internazionale tra autorità investigative e giudiziarie in materia di indagini informatiche*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- M. DANIELE, *Ricerca e formazione della prova*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;
- M. DANIELE, *Opposizione al riconoscimento dell'ordine europeo di sequestro e decisione de plano: una nullità assoluta*, in *Sistema penale*, 18 febbraio 2020;
- G. DARAIO, *Le rogatorie internazionali*, in AA.VV., *Trattato di procedura penale* (diretto da G. SPANGHER), vol. 6, *Esecuzione e rapporti con autorità giurisdizionali straniere* (a cura di L. KALB), Milanofiori Assago, 2009;
- G. DARAIO, *La circolazione della prova nello spazio giudiziario europeo*, in AA.VV., *«Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012;

- G. DARAIO, voce *Rogatorie internazionali*, in AA.VV., *Digesto del Processo penale* (diretto da A. SCALFATI), Torino, 2012;
- G. DARAIO, *Le rogatorie*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), IV, *Impugnazioni. Esecuzione penale. Rapporti con le autorità straniere* (a cura di L. KALB), Torino, 2015;
- G. DARAIO, *L'attuazione della d.q. 577/2003 sul reciproco riconoscimento dei provvedimenti di sequestro o di confisca*, in *Dir. pen. e proc.*, 9, 2016, p. 1133 ss.;
- G. DARAIO, *La raccolta transfrontaliera della prova penale nel costituendo spazio comune europeo di giustizia*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), Napoli, 2020;
- J. DASKAL, *The Un-Territoriality of Data*, in *The Yale Law Journal*, 2, 2015, p. 326 ss.;
- J. DASKAL, *Unpacking the CLOUD Act*, in *Eucrim*, 4, 2018, p. 220 ss.; ID., *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, in *Stanford Law Review Online*, 71, 2018, p. 9 ss.;
- J. DASKAL, *Privacy and Security Across Borders*, in *The Yale Law Journal Forum*, 128, 2019, p. 1029 ss.;
- J. DASKAL, P. SWIRE, *A Possible EU-US Agreement on Law Enforcement Access to Data?*, in *Lawfare*, 21 maggio 2018;
- J. DASKAL, P. SWIRE, *Why the CLOUD Act is Good for Privacy and Human Rights*, in www.justsecurity.org, 14 marzo 2018, p. 1 ss.;
- J. DASKAL, P. SWIRE, *The UK-US CLOUD Act Agreement is Finally Here, Containing New Safeguards*, in *Just Security*, 08 ottobre 2019;
- G. DE AMICIS, *Il mandato europeo di ricerca delle prove: un'introduzione*, in *Cass. pen.*, 7/8, 2008, p. 3033 ss.;
- G. DE AMICIS, *Limiti e prospettive del mandato europeo di ricerca della prova*, in penalecontemporaneo.it, 5 aprile 2011, p. 1 ss.;
- G. DE AMICIS, *All'incrocio tra diritti fondamentali, mandato d'arresto europeo e decisioni contumaciali: la Corte di Giustizia e il "caso Melloni"*, in penalecontemporaneo.it, 7 giugno 2013;
- G. DE AMICIS, *Dalle rogatorie all'ordine europeo di indagine: verso un nuovo diritto della cooperazione giudiziaria penale*, in *Cass. pen.*, 1, 2018, p. 22 ss.;
- G. DE AMICIS, *Prevalenza del diritto dell'Unione europea, delle convenzioni e del diritto internazionale in generale*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- G. DE AMICIS, *Gli organismi centralizzati della cooperazione giudiziaria: Eurojust*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;
- G. DE AMICIS, *La cooperazione orizzontale*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;
- F. DE ANGELIS, *L'espace judiciaire Pénal Européen: une vision se concrétise*, in *ERA Forum*, 1, supplement, 2011, p. 43 ss.;
- N. DE BOER, *Addressing rights divergences under the Charter: Melloni*, in *Common Market Law Review*, 4, 2013, p. 1083 ss.;
- A. DE CARO, voce *Giusto processo*, in *I dizionari sistematici, Procedura penale* (a cura di G. SPANGHER), Milano, 2008;

- G. DE DONATO, *L'attività del ministro della giustizia in tema di rogatorie attive e passive*, in AA.VV., *Rogatorie penali e sviluppi della cooperazione giudiziaria internazionale* (a cura di G. LA GRECA, M.R. MARCHETTI), Torino, 2003;
- A. DE FRANCESCO, *Inutilizzabili le rogatorie assunte all'estero in contrasto con le norme inderogabili di ordine pubblico e buon costume*, in *Dir e giust.*, 12 dicembre 2012;
- A. DE GUTTRY, *La circolazione transnazionale delle informazioni tra organi inquirenti su fatti di terrorismo*, in AA.VV., *Europa e terrorismo internazionale* (a cura di N. RONZITTI), Milano, 1992;
- A. DE GUTTRY, F. CAPONE, C. PAULUSSEN (eds.), *Foreign Fighters under International Law and Beyond*, The Hague, 2016;
- P. DE HERT, C. PARLAR, J. SAJFERT, *The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law*, in *Computer Law & Security Review*, 34, 2018, p. 327 ss.;
- P. DE HERT, J. THUMFART, *The Microsoft Ireland Case, the Cloud Act and the Cyberspace Sovereignty Trilemma*, in *Jusletter IT*, 12, 2021, p. 373 ss.;
- P. DE HERT, K. WEIS, N. CLOOSEN, *The Framework Decision of 18 December 2008 on the European Evidence Warrant for the Purpose of Obtaining Objects, Documents and Data for use in Proceedings in Criminal Matters – A Critical Assessment*, in *New Journal of European Criminal Law*, 2009, p. 55 ss.;
- D. DE JUDICIBUS, *TCP/IP*, in *Internet news*, 2, 1996, p. 74 ss.;
- P. DE LALLA, *La scelta del rito istruttorio*, Napoli, 1971;
- C. DE LUCA, *La prima pronuncia della Corte di giustizia sull'ordine europeo d'indagine penale: un approccio formale diretto a favorire l'efficacia della cooperazione giudiziaria*, in *Cass. pen.*, 10, 2020, p. 3854 ss.;
- S. DE LUCA, *La direttiva 2017/541/UE e il difficile bilanciamento tra esigenze di pubblica sicurezza e rispetto dei diritti umani*, in *Eurojus*, 3 luglio 2017;
- DE LISO, *"Naturalità" e "precostituzione" del giudice nell'art. 25 della Costituzione*, in *Giur. Cost.*, 1969, p. 2671 ss.;
- P. DE MARTINO, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico*, in *penalecontemporaneo.it*, 11 maggio 2015;
- P. DE SENA, *Dignità umana in senso oggettivo e diritto internazionale*, in *Diritti umani e diritto internazionale*, 3, 2017, p. 573 ss.;
- G. DE SIMONE, *La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*, in *penalecontemporaneo.it*, 28 ottobre 2012;
- G. DE VERO, *La responsabilità penale delle persone giuridiche*, in AA.VV., *Trattato di diritto penale* (diretto da C.F. GROSSO, T. PADOVANI, A. PAGLIARO), Milano, 2008;
- S. DE VRIES, E. BERNITZ, S. WEATHERILL (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument*, Abington, 2015;
- R. DEL COCO, *Ordine europeo di indagine e poteri sanzionatori del giudice*, in *penalecontemporaneo.it*, 21 dicembre 2015;
- D. DEL CORNO, *Introduzione a ESCHILO, Supplici, Prometeo incatenato*, Milano, 1994;
- C. DEL PRADO HIGUERA, E. SÁNCHEZ DE ROJAS DÍAZ, *Terrorismo islamista: El caso de Al Gama'a al Islamiya*, Valencia, 2018;

- F. DELLA CASA, G.P. VOENA, *Soggetti*, in AA.VV., *Compendio di procedura penale* (a cura di G. CONSO, V. GREVI, M. BARGIS), Milano, 2014;
- J. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della Corte di Giustizia UE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema Penale*, 29 aprile 2021;
- M.G.W. DEN BOER, *A diagnosis of the area of freedom, security and justice: remedies and reforms in the domains of immigration, terrorism and security*, in S. BLOCKMANS, S. PRECHAL (eds.), *Reconciling the deepening and widening of the European Union*, The Hague, 2007;
- D.E. DENNING, *Cyberterrorism: The Logic Bomb versus the Truck Bomb*, in *Global Dialogue*, 4, 2000, p. 29 ss.;
- D.E. DENNING, *Activism, Hacktivism and Cyberterrorism: The Internet as Tool for Influencing Foreign Policy*, in J. ARQUILLA, D. RONFELDT (eds.), *Networks and netwars. The influence of terror, crime and militancy*, Santa Monica, 2001;
- S. DEPAUW, *A European evidence (air)space? Taking cross-border legal admissibility of forensic evidence to a higher level*, in *European Criminal Law Review*, 1, 2016, p. 82 ss.;
- S. DEPAUW, *Electronic Evidence in Criminal Matters: How About E-Evidence Proposal*, in *European Criminal Law Review*, 1, 2018, p. 62 ss.;
- K.C. DESOUSA, T. HENSGEN, *Semiotic emergent framework to address the reality of cyberterrorism*, in *Technol. Forecast. Soc. Change*, 4, 2003, p. 388 ss.;
- V. DESTITO, voce *Reati informatici*, in *Dig. disc. pen.*, Agg. V, Torino, 2010, p. 739 ss.;
- M.L. DI BITONTO, *L'accentramento investigativo delle indagini sui reati informatici*, in *Dir. internet*, 5, 2008, p. 503 ss.;
- M.L. DI BITONTO, A. VITALE, A. MACRILLÒ, A. BARBIERI, E. FORLANI, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, in *Diritto dell'internet*, 5, 2008, p. 503 ss.;
- G. DI CHIARA, *Rapporti giurisdizionali con autorità straniera*, in *Enc. Dir.*, Agg. II, Milano, 1998;
- G. DI CHIARA, *Invio di documenti nella rogatoria internazionale*, in *Foro it.*, 10, 2002, p. 2564 ss.;
- G. DI DONATO, *Il cyberterrorismo di matrice religiosa*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- G. DI IEVA, G. ZAMBONINI, *Dal Surface al Dark Web, passando per il Deep Web (I parte)*, in *Sicurezza & Giust.*, 4, 2017, p. 49 ss.;
- G. DI PAOLO, «Tecnologie di controllo» e prova penale. *L'esperienza statunitense e spunti per la comparazione*, Padova, 2008;
- G. DI PAOLO, *Lo spazio di libertà, sicurezza e giustizia dell'UE: recenti novità sul fronte domestico e a livello europeo*, in *Cass. pen.*, 7/8, 2016, p. 3018C ss.;
- G. DI PAOLO, *La riforma della disciplina codicistica delle rogatorie internazionali (D.Lg. 3 ottobre 2017, n. 149)*, in *Cass. pen.*, 10, 2018, p. 3425 ss.;
- A. DI STASI, *Il diritto all'equo processo nella CEDU e nella Convenzione americana sui diritti dell'uomo. Analogie, dissonanze e profili di convergenza giurisprudenziale*, Torino, 2012;

- A. DI STASI, *Spazio europeo di libertà, sicurezza e giustizia e cooperazione giudiziaria in materia penale: il rispetto dei diritti fondamentali e della diversità tra ordinamenti nazionali e tradizioni giuridiche*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. Adattamenti normativi e approdi giurisprudenziali (a cura di L. KALB), Torino, 2012;
- A. DI STASI, *Rispetto dei diritti fondamentali e spazio europeo di giustizia: a proposito del Titolo VI della Carta dei diritti fondamentali*, in AA.VV., *I diritti umani nella giurisprudenza e nella prassi del diritto internazionale ed europeo* (a cura di L. PANELLA), Torino, 2013;
- A. DI STASI, *Introduzione alla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, Milano, 2018;
- A. DI STASI, *Human dignity as a normative concept: "dialogue" between European Courts (ECtHR and CJEU)?*, in P. PINTO DE ALBUQUERQUE, K. WOJTYCZEK (eds.), *Judicial power in a globalized world. Liber amicorum Vincent De Gaetano*, Cham, 2019, p. 115 ss.;
- A. DI STASI, *Il perfezionamento dello spazio europeo di libertà, sicurezza e giustizia: avanzamenti e criticità*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia* (a cura di A. DI STASI), Napoli, 2019;
- A. DI STASI, *L'incidenza virtuosa dei diritti fondamentali nel completamento dello Spazio europeo di giustizia*, in *Freedom security & justice Review*, 1, 2019, p. 1 ss.;
- A. DI STASI, *Tutela multilevel dei diritti fondamentali e costruzione dello spazio europeo di giustizia*, in AA.VV., *Tutela dei diritti fondamentali e spazio europeo di giustizia. L'applicazione giurisprudenziale del titolo VI della Carta* (a cura di A. DI STASI), Napoli, 2019;
- A. DI STASI, *CEDU e ordinamento italiano. La giurisprudenza della Corte europea dei diritti dell'uomo e l'impatto nell'ordinamento interno (2016-2020)*, II ed., Milano, 2020;
- A. DI STASI, *Parabola evolutiva della sovranità statale ed espansione delle competenze dell'Unione Europea: in particolare i limiti di applicabilità della Carta dei diritti fondamentali per gli Stati membri dell'Unione europea*, in AA.VV., *Liber Amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), Napoli, 2020;
- A. DI STASI, *The Enlargement of Competences of the European Union between State Sovereignty and the so-called European "Sovereignty": Focus on the limits of Applicability of the Charter of Fundamental Rights of the European Union*, in *Araucaria. Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, 3, 2020, p. 131 ss.;
- A. DI STASI, L.S. ROSSI (a cura di), *Lo spazio di libertà, sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere*, Napoli, 2020;
- A. DIDI, *La rimessione del processo penale*, Milano, 2000;
- A. DIDI, *Il regime delle intercettazioni telefoniche per «instradamento»*, in *Giust. pen.*, 3, 2001, p. 126 ss.;
- F.R. DINACCI, *Le regole generali delle prove*, in AA.VV., *Procedura penale. Teoria e pratica del processo*, (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), II, 2015;

- G. DIOTALLEVI, *La c.d. «concelebrazione» delle rogatorie e gli atti diretti di giurisdizione all'estero*, in *Cass. pen.*, 3, 1998, p. 913 ss.;
- G. DIOTALLEVI, sub *Art. 723*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- G. DIOTALLEVI, *Dalle rogatorie all'ordine di indagine europeo*, in AA.VV., *lo spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. DI STASI, L.S. ROSSI), Napoli, 2020;
- C. DOCKSEY, *Opinion 1/15 Privacy and security, finding the balance*, in *Maastricht Journal of European and Comparative Law*, 6, 2017, p. 768 ss.;
- D.P. DOMENICUCCI, F. FILPO, *La tutela giurisdizionale effettiva nel diritto dell'Unione europea*, in AA.VV., *Carta dei diritti fondamentali dell'Unione europea* (a cura di R. MASTROIANNI, O. POLLICINO, S. ALLEGREZZA, F. PAPPALARDO, O. RAZZOLINI), Milano, 2017;
- O. DOMINIONI, *In tema di nuova prova scientifica*, in *Dir. pen. Proc.*, 9, 2001, p. 1061 ss.;
- O. DOMINIONI, *La prova penale scientifica. Gli strumenti scientifico-tecnici nuovi o controversi e di elevata specializzazione*, Milano, 2005;
- O. DOMINIONI, *Il corpo del diritto delle prove*, in AA.VV., *Procedura penale*, Torino, 2017;
- L. DOMÍNGUEZ RUIZ, *La orden europea de investigación: el camino hacia un régimen europeo uniforme en materia de prueba penal*, in AA.VV., *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales* (F. JIMÉNEZ CONDE, Director), Valencia, 2018;
- O. DÖRR, K. SCHMALENBACH, *Vienna Convention on the Law of Treaties: a Commentary*, Heidelberg, 2012;
- U. DRAETTA, N. PARISI, *Elementi di diritto dell'Unione europea. Parte speciale*, IV ed., Milano, 2014;
- U. DRAETTA, N. PARISI, D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia dell'Unione europea: principi fondamentali e tutela dei diritti*, Napoli, 2007;
- T. DREIER, *Adjustment of Copyright Law to the Requirements of the Information Society*, in *IIC*, 6, 1998;
- G. DUCOLI, *La lotta dell'Unione europea al terrorismo. Un primo sguardo alla direttiva UE/2017/541*, in *Leg. Pen.*, 27 luglio 2017;
- W.H. DUTTON, *Society on the line*, Oxford, 1999;
- M. DWORSCHAK, *Auswirkungen von Schrems II auf den Steuerdatentransfer*, in *Liechtensteinische Juristen-Zeitung*, 2020, p. 295 ss.;
- M. EGAN, *What is the Dark Web? How to Access the Dark Web. What's the Difference Between the Dark Web and the Deep Web*, in *P.C. Advisor*, 23 novembre 2015;
- T.O. ELIAS, *The Modern Law of Treaties*, Leiden, 1974;
- M. ENDELMAN, *The Symbolic Uses of Politics*, Chicago, 1964;
- M. ENGELHARDT, *Heiliger Krieg, heiliger Profit. Afrika als neues Schlachtfeld des internationalen Terrorismus*, Berlin, 2014;
- T. EPIDENDIO, *Il caso Melloni: il nodo irrisolto del massimo standard di tutela dei diritti fondamentali*, in *Quaderni costituzionali*, 2, 2013, p. 451 ss.;

- J.A. ESPINA RAMOS, *The Relationship Between Eurojust and the European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018;
- V. ESPOSITO, voce *Rapporti giurisdizionali con autorità straniera*, in *Enc. Giur.*, XXV, Roma, 1991;
- EUROPEAN POLICE OFFICE (EUROPOL), *The Internet Organised Crime Threat Assessment (IOCTA) 2016*, The Hague, 2016;
- EUROPEAN POLICE OFFICE (EUROPOL), *European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017*, The Hague, 2017;
- EUROPEAN POLICE OFFICE (EUROPOL), *The Internet Organised Crime Threat Assessment (IOCTA) 2019*, The Hague, 2019;
- J. EYNARD, *D'une ingérence généralisée à une autre: deux poids, deux mesures?*, in *Revue trimestrielle des droits de l'homme*, 11, 2018 p.761 ss.;
- A. FABBRICATORE, *L'opposizione al riconoscimento dell'ordine europeo di sequestro probatorio*, in *Dir. Pen. e Proc.*, 6, 2020, p. 798 ss.;
- A. FABBRICATORE, *Effetti della ritardata comunicazione del decreto di riconoscimento dell'OEI*, in *Giur. It.*, 6, 2021, p. 1476 ss.;
- V. FAGGIANI, *La sentenza del TC sul caso Melloni: esempio del dialogo giudiziario europeo o di un monologo?*, in *forumcostituzionale.it*, 20 marzo 2015;
- F. FALATO, *Appunti di cooperazione giudiziaria penale*, Napoli, 2012;
- F. FALATO, *L'uso (preventivo e repressivo) dei dati personali come compressione di un diritto inviolabile*, in *Giust. pen.*, 10, 2016, p. 548 ss.;
- F. FALATO, *La proporzione innova il tradizionale approccio al tema della prova: luci ed ombre della nuova cultura probatoria promossa dall'ordine europeo di indagine penale*, in *Arch. pen.*, 1, 2018, p. 1 ss.;
- F. FALATO, *Appunti di cooperazione giudiziaria penale*, Napoli, 2019;
- V. FALCE, *Standard e Cloud computing*, in *Il diritto industriale*, 2 2015, p. 155;
- F. FALETTI, *The European Public Prosecutor's Office and the Principle of Equality*, in *Eucrim*, 1, 2017, p. 25 ss.;
- V. FANCHIOTTI, *Il dopo 11 settembre e l'Usa patriot act: lotta al terrorismo e «effetti collaterali»*, in *Quest. Giust.*, 2004, p. 283 ss.;
- I.V. FELCHER, *Una rassegna giurisprudenziale con riferimento alla Legge n. 48 del 2008 e alle investigazioni digitali*, in *Cyberspazio e diritto*, 1, 2013, p. 131 ss.;
- P. FELICIONI, *Le ispezioni e perquisizioni di dati e sistemi*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- T. FENUCCI, *A proposito della Corte di giustizia UE e dei c.d. "controlimiti": i casi Melloni e Taricco a confronto*, in *Freedom, Security & Justice Review*, 1, 2018, p. 95 ss.;
- L. FERRAJOLI, *La costruzione della democrazia. Teoria del garantismo costituzionale*, Bari-Roma, 2021;
- E. FERRI, G. GIACOBBE, G. TADDEI ELMI, *Informatica e ordinamento giuridico*, Milano, 1988;
- P. FERRUA, *Studi sul processo penale*, Torino, 1992;
- P. FERRUA, *Il "giusto processo" in Costituzione*, in *Dir. giust.*, 1, 2000, p. 78 ss.;
- P. FERRUA, *Il "giusto processo"*, Bologna, 2005;
- G. FIANDACA, *Il giudice di fronte alle controversie tecnico-scientifiche. Il diritto e il processo penale*, in *D.&Q. pubbl.*, 2005, p. 22 ss.;

- G. FIANDACA, G. LEINERI, sub *Art. 6 c.p.*, in AA.VV., *Commentario breve al codice penale* (a cura di G. FORTI, S. SEMINARA, G. ZUCCALÀ), VI ed., Milano, 2017;
- G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, Bologna, 2014;
- G. FIANDACA, E. MUSCO, *Diritto penale. Parte generale*, Bologna, 2019;
- M. FIDELBO, *La cooperazione rafforzata come modalità d'istituzione della procura europea*, in *Riv. dir. pen. cont.*, 3, 2016, p. 92 ss.;
- L. FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *Penale Diritto e Procedura*, 1 ottobre 2021, p. 1 ss.;
- G. FIORELLI, *I motivi di rifiuto dell'ordine investigativo europeo, quando "fidarsi è bene, ma non fidarsi è meglio"*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016;
- J. FISHER, *Draft Convention on Cybercrime: Potential Constitutional Conflicts*, in *University West Las Angeles Review*, 2001, p. 339 ss.;
- M. FLETCHER, E. HERLIN-KARNELL, C. MATERA (eds.), *The European Union as an Area of Freedom, Security and Justice*, London e New York, 2016;
- E. FLETT, J. WILSON, J. CLOVER, *Schrems strikes again: EU-US privacy shield suffers same fate as its predecessor*, in *Computer and Telecommunications Law Review*, 2020, p. 161 ss.;
- R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. e proc. pen.*, 2/3, 2007, p. 899 ss.;
- R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *Diritto penale contemporaneo*, 20 settembre 2012;
- R. FLOR, *La Corte di Giustizia considera la Direttiva europea 2006/24 sulla c.d. "data retention" contraria ai diritti fondamentali. Una lunga storia a lieto fine?*, in *Dir. pen. cont.*, 2, 2014, p. 178 ss.;
- R. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. e proc.*, 10, 2015, p. 1291 ss.;
- R. FLOR, *Il contrasto al terrorismo nell'era delle nuove tecnologie e i meccanismi di cooperazione fra settore pubblico e settore privato*, in AA.VV., *Scritti in onore di Luigi Stortoni* (a cura di M. MANTOVANI, F. CURI et al.), Bologna, 2016;
- R. FLOR, *Cyber-terrorismo e diritto penale in Italia*, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali* (a cura di R. WENIN, G. FORNASARI), Napoli, 2017;
- R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata questio (?)*, in *penalecontemporaneo.it*, 29 marzo 2017;
- R. FLOR, *Cybercriminality: le foti internazionali ed europee*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- D. FLORE, *La notion de confiance mutuelle: l'"alpha" ou l'"omega" d'une justice pénale européen*, in AA.VV., *La confiance mutuelle dans l'espace pénal européen* (a cura di G. DE KERCHOVE, A. WEYEMBERGH), Bruxelles, 2005;
- L. FLORIDI, *Infosfera: etica e filosofia nell'età dell'informazione*, Torino, 2009;

- L. FLORIDI, *La quarta rivoluzione: come l'infosfera sta trasformando il mondo*, Milano, 2017;
- C. FORGET, *L'avis de la C.J.U.E. sur l'accord PNR Union européenne-Canada: une occasion ratée de réaffirmer le principe de finalité?*, in *Journal de droit européen*, 247, 2018, p.87 ss.;
- G. FORTINO, P. TRUNFIO, *Internet of Things Based on Smart Objects*, Berlino, 2004;
- G. FOSCHINI, *Giudice naturale e costituzione del giudice*, in G. FOSCHINI, *Tornare alla giurisdizione. Saggi critici*, Milano, 1971;
- V. FRANSSEN, *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?*, in *European Data Protection Law Review*, 3, 2017, p. 534 ss.;
- N. FRANSSEN, *The Future Judicial Cooperation between the EPPO and Non-Participating Member States Editorial*, in *New Journal of European Criminal Law*, 2018, p. 291 ss.;
- V. FRASSEN, *The European Commission's e-Evidence Proposal: toward an EU-wide obligation for service providers to cooperate with law enforcement?*, in www.europeanlawblog.eu, 12 ottobre 2018;
- L. FROMONT, A. VAN WAEYENBERGE, *La protection jurisdictionnelle effective en Europe ou l'histoire d'une procession d'Echternac*, in *Chaiers de droit européenne*, 1, 2015, p. 115 ss.;
- T.E. FROSINI, *Libertè, Egalità, Internet*, II ed., Napoli, 2019;
- T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Il diritto dell'informazione e dell'informatica*, 3, 2020, p. 465 ss.;
- V. FROSINI, *Il diritto nella società tecnologica*, Milano, 1980;
- V. FROSINI, *Telematica ed informatica giuridica*, in *Enc. dir.*, XLIV, Milano, 1992;
- V. FROSINI, *Informatica, diritto e società*, Milano, 1992;
- V. FROSINI, *La criminalità informatica*, in *Il dir. dell'informazione e dell'informatica*, 3, 1997, p. 487 ss.;
- H. FIJITA, A. GAETA, V. LOIA, F. ORCIUOLI, *Hypotheses Analysis and Assessment in Counterterrorism Activities: A Method Based on OWA and Fuzzy Probabilistic Rough Sets*, in *IEEE Transactions on Fuzzy Systems*, 28, 2020, p. 831 ss.;
- B. FURHT, A. ESCALANTE (a cura di), *Handbook of Cloud Computing*, New York, Dordrecht, Heidelberg, London, 2010;
- S. FURNELL, *Cyber crime: Vandalizing the Information Society*, Boston, 2002;
- C. GABRIELLI, *Costituzionalmente legittima la disciplina dell'ascolto protetto del minore: un approdo condivisibile, al di là di qualche ambiguità argomentativa*, in *Giurisprudenza costituzionale*, 2, 2018, p. 815C ss.;
- C. GABRIELLI, *La disciplina dell'esame del minore in incidente probatorio regge alle censure di incostituzionalità*, in *Riv. it. Dir. e proc. pen.*, 2, 2018, p. 964 ss.;
- A. GAITO, *Dei rapporti giurisdizionali con autorità straniera*, Padova, 1985;
- A. GAITO, *Spazio penale europeo e cooperazione giudiziaria internazionale*, in AA.VV., *Procedura penale*, Torino, 2019;
- A. GAITO, *Mandato di arresto europeo ed estradizione*, in AA.VV., *Procedura penale*, Torino, 2020;

- N. GALANTINI, *La cooperazione internazionale per la ricerca e l'acquisizione della prova*, in AA.VV., *Argomenti di procedura penale internazionale* (a cura di O. DOMINIONI), Milano, 1982;
- N. GALANTINI, *Una nuova dimensione per il ne bis in idem internazionale*, in *Cass. pen.*, 10, 2004, p. 3474 ss.;
- J. GALBRAITH, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, in *The American Journal of International Law*, 3, 2018, p. 486 ss.;
- J. GALBRAITH, *United States and United Kingdom Sign the First Bilateral Agreement Pursuant to the CLOUD Act, Facilitating Cross-Border Access to Data*, in *American Journal of International Law*, 1, 2020, p. 124 ss.;
- P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997;
- L. LUPÁRIA, *Computer crimes e procedimento penale*, in AA.VV., *Trattato di procedura penale* (a cura di G. GARUTI), Torino, 7, I, 2011;
- B. GALGANI, *Assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- B. GALGANI, *Giudizio penale, habeas data, e garanzie fondamentali*, in *Arch. pen.*, 1, 2019, p. 1 ss.;
- B. GALGANI, *Digitalizzazione e processo penale*, in *Questione giustizia*, 19 gennaio 2021;
- M. GALLO, *Capacità penale*, in *Nov. Dig. it.*, vol. II, Torino, 1958;
- N. GALLO, *L'attività di contrasto al terrorismo di matrice islamica. Le scelte del legislatore*, in AA.VV., *Conflittualità politico sociale intorno al Mediterraneo* (a cura di A. PANAINO), Milano, 2006;
- A. GAMBARO, R. SACCO, *Sistemi giuridici comparati*, Torino, 2009;
- A.M. GAMBINO, *Gli scambi in rete*, in *Il dir. dell'informazione e dell'informatica*, 2, 1997, p. 423 ss.;
- A. GAMBINO, A. STAZI, D. MULA, *Diritto dell'informatica e della comunicazione*, Torino, 2019;
- R. GAROFOLI, *Manuale di diritto penale*, Roma, 2017;
- S. GÁSPÁR-SZILÁGYI, *Joined Cases Aranyosi and Caldáraz: Converging Human Rights Standards, Mutual Trust and a New Ground for Postponing a European Arrest Warrant*, in *European journal of Crime, criminal Law and criminal Justice*, 24, 2016, p. 197 ss.;
- C. GATTEI, *Tutela dell'opera multimediale su rete telematica: la situazione europea*, in *Dir. Informatica*, 2, 1998, p. 469 ss.;
- E. GATTO, *Il principio di proporzionalità nell'ordine europeo di indagine penale*, in *dir. pen. cont.*, 2, 2019, p. 69 ss.;
- A. GAUDIERI, *La nuova Agenzia dell'Unione europea per la cooperazione giudiziaria penale (Eurojust)*, in *Osservatorio SLSG*, novembre 2018;
- A. GAUDIERI, *Mandato di arresto europeo: la Corte di Giustizia si pronuncia sul delicato tema della sospensione della misura detentiva ai fini della consegna*, in *smsg.unisa.it*, febbraio 2019;
- A. GAUDIERI, *Estorsione via chat e gravi indizi di colpevolezza nel procedimento penale*, in *Diritto di internet*, 2, 2019, p. 141 ss.;

- A. GAUDIERI, *Corte cost., 21 febbraio – 27 aprile 2018, n. 92*, in AA.VV., *Corte costituzionale e sistema processuale penale. L'elaborazione giurisprudenziale del 2018* (a cura di D. CIMADOMO, G. DALIA), Milano, 2019;
- A. GAUDIERI, *Conformità del rapporto di subordinazione del pubblico ministero con la direttiva 2014/41/UE: l'orientamento adottato dalla Corte di giustizia nella sentenza A. e A.*, in *slsg.unisa.it*, dicembre 2020, p. 1 ss.;
- A. GAUDIERI, *Opposizione al decreto di riconoscimento dell'ordine europeo di sequestro: scenari*, in *Giur. It.*, 8-9, 2020, p. 2033 ss.;
- A. GAUDIERI, *Sovraffollamento carcerario: i criteri dettati dalla sentenza Dorobantu per il calcolo degli spazi. Una "bussola" per le scelte da compiere in periodo di emergenza sanitaria?*, in *Freedom, Security & Justice Review*, 2, 2020, p. 213 ss.;
- M. GEBAUER, F. BERNER, *Ordre Public (Public Policy)*, in *Max Planck Encyclopedias of International Law*, agosto 2019;
- R.M. GERACI, *La circolazione transfrontaliera delle prove digitali in UE: la proposta di Regolamento e-evidence*, in *Cass. pen.*, 3, 2019, p. 1340 ss.;
- R.M. GERACI, *Ordine europeo di indagine ricevuto dall'estero e rimedi impugnatori praticabili*, in *Cass. pen.*, 9, 2019, p. 3184 ss.;
- M. GERCKE, *10 years Convention on Cybercrime: Achievements and Failures of the Europe's Instrument in the Fight against Internet-related Crimes*, in *Computer Law Review International*, 5, 2011, p. 142 ss.;
- M. GEROSA, *Second Life*, Milano, 2007;
- A. GHIRARDINI, G. FAGGIOLI, *Computer forensics*, Milano, 2007;
- M. GIACOMETTI, S. NEVEU, *La décision d'enquête européenne: un nouvel instrument destiné à révolutionner la récolte de preuves au sein de l'UE?*, in *Revue de Droit pénal et de Criminologie*, 9-10, 2016, p. 899 ss.;
- M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre del risk assessment tools tra Stati Uniti ed Europa*, in *Dir. pen. cont.*, 29 maggio 2009;
- M. GIALUZ, J. DELLA TORRE, *Lotta alla criminalità nel cyberspazio: la Commissione presenta due proposte per facilitare la circolazione delle prove elettroniche nei processi penali*, in *Dir. pen. cont.*, 5, 2018, p. 277 ss.;
- M. GIALUZ, E. GRISONICH, *Crisi dell'Unione europea e crepe nel reciproco riconoscimento: il dialogo costruttivo tra le Corti assicura il rispetto dei diritti fondamentali e l'efficacia del mandato di arresto europeo*, in *Cass. pen.*, 7-8, 2020, p. 2669 ss.;
- A. GIARDA, *Un decennio di giustizia penale europea prima del Trattato di Lisbona*, in AA.VV., *I nuovi orizzonti della giustizia penale europea*, Atti del convegno ASPP, Milano, 24-26 ottobre 2014, Milano, 2015;
- A.H. GIBBS, *Thinking constitutionally about the European Union's area of freedom, security and justice*, Thesis – European University Institute, 2009;
- A.H. GIBBS, *Constitutional Life and Europe's Area of Freedom Security and Justice*, England-USA, 2013;
- W. GIBSON, *Neuromancer*, New York, 1984;
- L. GIORDANO, *L'intercettazione delle e-mail (già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze"*, in *ilpenalista.it*, 14 novembre 2016;

- L. GIORDANO, *Intercettazioni: è al tramonto la stagione dell'instradamento?*, in *ilpenalista.it*, 12 giugno 2017;
- L. GIORDANO, *La direttiva OEI e la disciplina delle intercettazioni "transfrontaliere": è alla fine la stagione dell'instradamento?*, in *La Magistratura*, 3, 2017, p. 93 ss.;
- L. GIORDANO, *Captatore informatico: utilizzabili anche le conversazioni intercettate all'estero*, in *ilprocessotelematico.it*, 18 dicembre 2020;
- L. GIORDANO, *La Corte di Cassazione ritorna sull'acquisizione dei tabulati telefonici dopo le indicazioni della CGUE*, in *ilPenalista.it*, 5 ottobre 2021;
- G. GIOSTRA, *Prima lezione sulla giustizia penale*, Bari-Roma, 2020;
- C. GITTARDI, *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *Giustizia insieme*, 7 ottobre 2021, p. 1 ss.;
- F. GIUFFRIDA, *Cross-Border Crimes and the European Public Prosecutor's Office*, in *Eucrim*, 3, 2017, p. 149 ss.;
- S. GLESS, *Zum prinzip der gegenseitigen Anerkennung*, in *ZStW*, 2004;
- S. GLESS, *Strategie e tecniche per l'armonizzazione della prova*, in AA.VV., *Prova penale e Unione europea* (a cura di G. ILLUMINATI), Bologna, 2009, p. 141 ss.;
- M. GNES, E. CHITI, *Cronache europee 2014*, in *Riv. trim. dir. pubbl.*, 3, 2015, p. 1047 ss.;
- M. GNES, E. CHITI, *Cronache europee 2015*, in *Riv. trim. dir. pubbl.*, 4, 2016, p. 1113 ss.;
- T.W. GOLDSMITH, *Who Controls the Internet? Illusions of a Borderless World*, New York, 2006;
- L. GÓMEZ AMIGO, *Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima*, in *Revista Española de Derecho Europeo*, 71, 2019, p. 23 ss.;
- S. GORDON, R. FORD, *Cyberterrorism? Symantec Security Response White Paper*, Cupertino, 2003;
- S. GOSWAMI, *Internet protocols. Advances, Technologies and Applications*, Berlino, 2003;
- A. GRANELLI, *Il sé digitale*, Milano, 2006;
- G. GRASSO, *La cooperazione giudiziaria in materia penale tra gli Stati membri delle Comunità europee*, in *Foro it.*, 4, 1987, p. 458 ss.;
- F. GRAZIANI, *L'acquisizione della prova digitale all'estero: verso un secondo Protocollo addizionale alla Convenzione di Budapest sul cybercrime*, in AA.VV., *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa* (a cura di S. MARCHISIO, U. MONTUORO), Torino, 2019;
- F. GRAZIANI, *La ricerca della prova digitale mediante captatore informatico nella prassi degli Stati e nell'ordinamento italiano: il difficile equilibrio tra prevenzione dei reati e tutela della riservatezza informatica*, in *La Com. int.*, 3, 2019, p. 391 ss.;
- V. GREVI, *Commento all'art. 9 l. 28/7/1984 n. 398*, in *Leg. pen.*, 1985;
- V. GREVI, G. ILLUMINATI, *Prove*, in AA.VV., *Compendio di procedura penale* (a cura di G. CONSO, V. GREVI e M. BARGIS), Padova, 2018;
- L.K. GROSSMAN, *The Electronic Republic. Reshaping Democracy in the Information Age*, New York, 1995;

- C.F. GROSSO, *Su di un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, in *Riv. it. dir. e proc. pen.*, 3, 2014, p. 1518 ss.;
- V.R. GRUNDMAN, *The New Imperialism: The Extraterritorial Application of United States Law*, in *The International Lawyer*, 14, 1980, p. 257 ss.;
- P. GUALTIERI, *Prova informatica e diritto di difesa*, in *Diritto penale e processo*, 4, 2011, p. 493 ss.;
- U. GUERINI, *Il terzo pilastro dell'Unione europea: uno spazio di libertà, sicurezza e giustizia*, in AA.VV., *Il diritto penale dell'Unione europea. La normativa, la dottrina, la giurisprudenza europea in materia penale e la cooperazione giudiziaria*, Torino, 2008;
- E. GUILD, F. GEYER, *Security Versus Justice? Police and Judicial Cooperation in the European Union*, Great Britain, 2013;
- E. GUILD, E. MENDOS KUŞKONMAZ, *EU Exclusive jurisdiction on surveillance related to terrorism and serious transnational crime: case review on opinion 1/15*, in *European Law Review*, 4, 2018, p. 583 ss.;
- E. GUILD, E. MENDOS KUŞKONMAZ, *A critical take on opinion 1/15: is the glass half full or half empty?*, in AA.VV., *European yearbook on human rights* (P. CZECH, L. HESCHL, K. LUKAS, M. NOWAK, G. OBERLEITNEIR eds.), Cambridge, 2019;
- P. HÄBERLE, *Le libertà fondamentali nello Stato costituzionale*, (1983), trad. it., Roma, 1993;
- K. HAFNER, M. LYON, *Where Wizards Stay up Late: The Origins of the Internet*, New York, Touchstone, 1998;
- A. HARATSCH, S. SCHMAHL, *Die Anwendung ratione temporis der Wiener Konvention über das Recht der Verträge*, in *Zeitschrift für Öffentliches Recht*, 2003, p. 105 ss.;
- T.I. HARBO, *Introducing procedural proportionality review in European Law*, in *Leiden Journal of International Law*, 1, 2017, p. 25 ss.;
- G. HARPAZ, *Common Foreign and Security Policy, counter-terrorism measures and judicial review: Hamas and LTTE*, in *Common Market Law Review*, 6, 2018, p. 1917 ss.;
- V. HATZOPOULOS, *Le principe communautaire d'équivalence et de reconnaissance mutuelle dans la libre prestation de services*, Athènes-Bruxelles, 1999;
- B. HE, M. PATEL, Z. ZHANG, K. CHEN-CHUAN CHANG, *Accessing the Deep Web: A Survey*, Comm. ACM, 2007;
- B. HECKER, *Mutual Recognition and the Transfer of Evidence. The European Evidence Warrant*, in AA.VV., *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (coordinato da S. RUGGERI), Heidelberg, 2013;
- R. HEINSCH, *Foreign Fighters and International Criminal Law*, in A. DE GUTTRY, F. CAPONE, C. PAULUSSEN (eds.), *Foreign Fighters under International Law and Beyond*, The Hague, 2016;
- D. HELENIUS, *Mutual Recognition in Criminal Matters and the Principle of Proportionality. Effective Proportionality or Proportionate Effectiveness?*, in *New Journal of European Criminal Law*, 3, 2014, p. 349 ss.;
- E. HERLIN-KARNELL, *The domination of security and the promise of justice: on justification and proportionality in Europe's Area of Freedom, Security and Justice*, in *Transnational Legal Theory*, 1, 2017, p. 79 ss.;

- H. HIJMANS, *PNR Agreement EU-Canada Scrutinised: CJEU Gives Very Precise Guidance to Negotiators*, in *European Data Protection Law Review*, 3, 2017, p. 406 ss.;
- S.B. HOAR, *Trend in cybercrime: the dark side of the internet*, in *Criminal Justice*, 3, 2005, p. 4 ss.;
- H. HOFFMAN, *Sub art. 47. Right to an Effective Remedy. Specific Provisions (Meaning)*, in AA.VV., *The EU Charter of Fundamental Rights. A Commentary* (a cura di S. PEERS, T. HERVEY, J. KENNER, A. WARD eds.), Oxford, 2014;
- R.L. HOLZHACKER, P. LUIF, *Freedom, Security and Justice in the European Union: Internal and External Dimensions of Increased Cooperation After the Lisbon Treaty*, New York, 2014;
- W.K. HON, C. MILLARD, I. WALDEN, *Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now*, in *Stanford Technology Law Review*, 2012, p. 83 ss.;
- L. HUEY, R. ROSENBERG, *Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention*, in *Canadian Journal of Criminology and Criminal Justice*, 5, 2004, p. 597 ss.;
- R. HÜLSSE, A. SPENCER, *The Metaphor of Terrorism: Terrorism Studies and the Constructivist Turn*, in *Security Dialogue*, 6, 2008, p. 571 ss.;
- I. IAI, *Rogatoria eseguita all'estero dall'autorità giurisdizionale dello Stato richiedente*, in *Giur. It.*, 7, 2000, p. 1471 ss.;
- A. IERMANO, *La tutela delle vittime di reato nello "spazio procedural-processuale penale": la direttiva 2012/29/UE*, in *Rivista della cooperazione giuridica internazionale*, 45, 2013, p. 125 ss.;
- A. IERMANO, *Garanzie minime nello spazio europeo di giustizia penale*, Napoli, 2014;
- A. IERMANO, *Sistema globale di acquisizione delle prove nelle fattispecie aventi dimensione transfrontaliera: l'ordine europeo di indagine penale (OEI)*, in *Diritto comunitario e degli scambi internazionali*, 3-4, 2015, p. 483 ss.;
- A. IERMANO, *La nozione di pena tra forma e sostanza nel sistema di tutela europeo*, Bari, 2018;
- A. IERMANO, *Verso un nuovo diritto "fondamentale" in ambito UE: il diritto alla disconnessione digitale*, in *Eurojus*, 2, 2021, p. 150 ss.;
- C. IASEVOLI, *La nullità nel sistema processuale penale*, Napoli, 2008;
- F. IOVENE, *"Data retention" tra passato e futuro. Ma quale presente?*, in *Cass. pen.*, 12, 2014, p. 4274 ss.;
- F.P.C. IOVINO, *Effetti del reciproco riconoscimento per l'esecuzione delle misure di sospensione condizionale delle sanzioni sostitutive*, in *Dir. pen. e proc.*, 9, 2016, p. 1148 ss.;
- B. ISENRING, R.D. MAYBUD, L. QUIBLIER, *Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick*, in *Schweizerische Juristen-Zeitung*, 2019, p. 445 ss.;
- F. JACQUES, *«Uncle Sam is watching you» Retour sur les enseignements de l'arrêt Schrems II de la Cour de justice de l'Union européenne*, in *Journal des tribunaux*, 2021, p. 246 ss.;
- R. JANSEN, *Explaining the methods for taking evidence abroad within the EU and some first observations on the proposal for the Evidence Regulation (recast)*, in *Nederlands Internationaal Privaatrecht*, 4, 2019, p. 753 ss.;

- C. JANSSENS, *The Principle of Mutual Recognition in EU Law*, Oxford, 2013;
- F. JAULT-SESEKE, J. LELIEUR, C. PIGACHE (eds.), *L'espace judiciaire européen civil et pénal: regards croisés: actes du 25e colloque des Instituts d'études judiciaires, 20-21 mars 2009 à l'Université de Rouen*, Paris, 2009;
- C. JEFFRAY, T. FEAKIN, *Underground web: The cybercrime challenge*, in *Australian Strategic Policy Institute*, marzo 2015, p. 1 ss.;
- J.H. JEPPESEN, G. NOJEIM, *Initial Observations on the European Commission's e-Evidence Proposals*, in *www.cdt.org*, 18 aprile 2018;
- J.H. JEPPESEN, G. NOJEIM, *Assessing the European Commission's E-Evidence Proposals on Ten Human Rights Criteria*, in *www.cdt.org*, 18 aprile 2018;
- M. JIMENO BULNES, *Orden europea de investigación en materia penal*, in AA.VV., *Aproximación legislativa versus reconocimiento mutuo en el desarrollo del espacio judicial europeo: una perspectiva multidisciplinar* (M. JIMENO BULNES, Directora), Barcellona, 2016;
- R. JURKA, *Movement of evidence in the European Union: Challenges for the European Investigation Order*, in *Baltic Journal of Law & Politics*, 2, 2016;
- L. KALB, *Il processo per le imputazioni connesse*, Torino, 1990;
- L. KALB, *Il documento nel sistema probatorio*, Torino, 2000;
- L. KALB, *La "ricostruzione orale" del fatto tra "efficienza" ed "efficacia" del processo penale*, Torino, 2005;
- L. KALB (a cura di), *Mandato d'arresto europeo e procedure di consegna. Commento alla legge 22 aprile 2005, n.69*, Milano, 2005;
- L. KALB, *L'effettività del diritto alla traduzione degli atti dopo la Dir. 2010/64/UE*, in *Giur. It.*, 1, 2014, p. 714 ss.
- L. KALB, *Procedimenti «paralleli» e giurisdizione «concordata»: il nuovo quadro normativo sul trasferimento dei procedimenti penali (nello spazio europeo e in quello internazionale)*, in *Arch. pen.*, 1, speciale riforme, 2018, p. 799 ss.;
- L. KALB, *Commento agli artt. 10-17 d. legisl. 7 agosto 2015, n. 137 (Attuazione della decisione quadro 2006/783/GAI relativa all'applicazione del principio del reciproco riconoscimento delle decisioni di confisca)*, in AA.VV., *Commentario breve al Codice antimafia e alle altre procedure di prevenzione* (a cura di G. SPANGHER, A. MARANDOLA), Milano, 2019;
- L. KALB, *Introduzione*, in AA.VV., *Diritti della persona e nuove sfide del processo penale*. Atti del XXXII Convegno nazionale ASPP – Salerno, 25-27 ottobre 2018 (a cura di L. KALB), Milano, 2019;
- L. KALB, *Emergenza sanitaria e giustizia penale. Un'analisi delle misure incidenti sul sistema processuale penale*, in *Dir. pen. e proc.*, 7, 2020, p. 910 ss.;
- L. KALB, *Gli insegnamenti di un Maestro per lo studio delle nuove sfide: l'istituzione della Procura europea*, in AA.VV., *Liber amicorum per Massimo Panebianco* (a cura di A. DI STASI, G. FAUCEGLIA, G. MARTINO, P. PENNETTA), Napoli, 2020;
- L. KALB, *Questioni problematiche in tema di Procura europea*, in AA.VV., *Lo spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. DI STASI, L.S. ROSSI), Napoli, 2020;
- L. KALB, sub Art. 746 bis – 746 quater c.p.p., in AA.VV., *Commentario breve al codice di procedura penale* (a cura di G. ILLUMINATI, L. GIULIANI), Milano, 2020, p. 3571 ss.;

- L. KALB, *Codice di procedura penale. Coordinato con le norme complementari*, Milano, 2021;
- L. KALB, I. IZZO, *La nuova sfida della direttiva 2010/64: un'assistenza linguistica di "qualità" per lo svolgimento di un procedimento effettivamente "equo"*, in AA.VV., in «Spazio europeo di giustizia» e procedimento penale italiano (a cura di L. KALB), Torino, 2012;
- L. KALB, S. NEGRI, *The Criminal Justice Response to Organ Trafficking and Trafficking in Human Beings for Organ Removal*, in *Journal of Trafficking and Human Exploitation*, 2, 2017, p. 187 ss.;
- H. KELSEN, *La dottrina pura del diritto*, Torino, 1966;
- G. KENT, *Sharing Investigation-Specific Data with Law Enforcement – An International Approach*, in *Stanford Public Law Working Paper*, 2014;
- G. KENT, *The Mutual Legal Assistance Problem Explained*, in CIS Blog – The Center for Internet and Society, 23 febbraio 2015;
- O.S. KERR, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, in *George Washington Law Review*, 72, 2004, p. 1208 ss.;
- O.S. KERR, *The Next Generation Communications Privacy Act*, in *University of Pennsylvania Law Review*, 2, 2014, p. 373 ss.;
- O.S. KERR, *Computer Crime Law*, Thomson West, St. Paul MN, 2018;
- M. KEYSER, *The Council of Europe Convention on Cybercrime*, in *J. Transnational Law & Policy*, 2, 2003, p. 287 ss.;
- E.B. KIM, *U.S.-U.K. Executive Agreement: Case Study of Incidental Collection of Data Under the CLOUD Act*, in *Washington Journal of Law, Technology & Arts*, 3, 2020, p. 247 ss.;
- J. KLAUSEN, *Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq*, in *Studies in Conflict & Terrorism*, 1, 2015, p. 1 ss.;
- L. KLIMEK, *Free movement of evidence in criminal matters in the EU*, in *The Lawyer Quarterly*, 4, 2012, p. 265 ss.;
- L. KLIMEK, *Mutual recognition of Judicial Decisions in European Criminal Law*, Berlino, 2017;
- A. KLIP, *European Criminal Law. An Integrative Approach*, Cambridge, 2021;
- R.K. KNAKE, *Weaponizing Digital Trade. Creating a Digital Trade Zone to Promote Online Freedom and Cybersecurity*, Council on Foreign Relations, New York, 2020;
- B.J. KOOPS, M. GOODWIN, *Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law*, Tilburg, 2014;
- E.J. KOOPS, T. ROBINSON, *Cybercrime Law: A European Perspective Crime*, in E. CASEY (ed.), *Digital Evidence and Computer Crime*, III ed., Waltham, 2011;
- T. KOSTAKOPOULOU, *The area of freedom, security and justice and the European Union's constitutional dialogue*, in C. BARNARD (ed.), *The fundamentals of EU law revisited*, USA, 2007;
- R.E. KOSTORIS, *Il nuovo "pacchetto" antiterrorismo, tra prevenzione, contrasto in rete e centralizzazione delle indagini*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo* (a cura di R. KOSTORIS, F. VIGANÒ), Torino, 2015;

- R.E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in AA.VV., *I nuovi orizzonti della giustizia penale europea. Atti del convegno. Milano, 24-26 ottobre 2014*, Milano, 2015;
- R. E. KOSTORIS, *Processo penale, diritto europeo e nuovi paradigmi del pluralismo giuridico postmoderno*, in *Riv. it. dir. e proc. pen.*, 3, 2015, p. 1177 ss.;
- R.E. KOSTORIS, *L'OEI nella dissolvenza tra regole e principi*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- R.E. KOSTORIS, *Ordine di investigazione europeo e tutela dei diritti fondamentali*, in *Cass. pen.*, 5, 2018, p. 1437 ss.;
- R.E. KOSTORIS, *Processo penale e paradigmi europei*, Torino, 2018;
- R.E. KOSTORIS, *Diritto europeo e giustizia penale*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;
- R.E. KOSTORIS, *Gli organismi centralizzati della cooperazione giudiziaria: la Procura europea*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;
- R.E. KOSTORIS, R. ORLANDI, *Introduzione*, in AA.VV., *Contrasto al terrorismo interno e internazionale* (a cura di R.E. KOSTORIS, R. ORLANDI), Torino, 2006;
- F. KRAMER, S. STARR, L. WENTZ (eds), *Cyberpower and National Security*, Washington (D.C.), 2009;
- F. KRENEC, *Article 47. Droit à un recours effectif et à accéder à un tribunal impartial*, in AA.VV., *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article* (F. PICOD, S. VAN DROOGHENBROECK eds.), Bruxelles, 2018;
- V. KRISHNAMURTHY, *Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters*, in *The Berkman Klein Center for Internet & Society Research Publication*, 3, 2016, p. 1 ss.;
- D.T. KUEHL, *From Cyberspace to Cyber-power: Defining the Problem*, in F. KRAMER, S. STARR, L. WENTZ (eds.), *Cyberpower and National Security*, Washington (D.C.), 2009;
- C. KUNER, *International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 3, 2018, p.857 ss.;
- N. KUSHWAHA, P. ROGUSKI, B.W.WATSON, *Up in the Air: Ensuring Government Data Sovereignty in the Cloud*, in AA.VV., *2020 12th International Conference on the Cyber Conflict (CyCon)* (T. JANČÁRKOVÁ, L. LINDSTRÖM, M. SIGNORETTI, I. TOLGA, G. VISKY eds.), Tallin, 2020;
- F. LA CHIOMA, *L'ordine di produzione e di conservazione europeo delle prove elettroniche*, in *magistraturaindipendente.it*, 6 giugno 2019;
- K. LA REGINA, *Le indagini su dispositivi digitali*, in AA.VV., *Investigazioni digitali* (a cura di M. IASELLI), Milano, 2020;
- E.N. LA ROCCA, *Dalla "libera circolazione dei soggetti" alla "libera circolazione del materiale probatorio": la Decisione-Quadro sul mandato europeo di ricerca delle prove*, in *Osservatorio del processo penale*, 2007, p. 37 ss.;
- E.N. LA ROCCA, *Intercettazioni, utilizzo di impianti esterni, instradamento: garanzie tecniche e prassi devianti*, in *Giur. It.*, 3, 2011, p. 731 ss.;

- E.N. LA ROCCA, *Le regole di esclusione della prova nel processo penale*, Roma, 2013;
- E.N. LA ROCCA, *La legge di ratifica ed esecuzione della Convenzione di assistenza giudiziaria in materia penale tra gli Stati membri Ue*, in *Arch. pen.*, 3, 2016, p. 1 ss.;
- H. LABAYLE, *La nouvelle architecture de l'espace de liberté, de sécurité et de justice*, in C. KADDOUS, M. DONY (eds.), *D'Amsterdam à Lisbonne*, Bruxelles, 2010;
- H. LABAYLE, *Mandat d'arrêt européen et degré de protection des droits fondamentaux, quand la confiance se fait aveugle*, in *gdr-elsj.eu*, 3 marzo 2013;
- S. LABRIOLA, *I fini dello Stato e l'umanità plurale*, in AA.VV., *Ripensare lo Stato* (a cura di S. LABRIOLA), Milano, 2003;
- W. LACSON, B. JONES, *The 21st Century DarkNet Market: Lessons from the Fall of Silk Road*, in *International Journal of Cyber Criminology*, 1, 2016, p. 40 ss.;
- V. LAGI, *Deep web, dark web e indagini informatiche*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- M. LAKOMY, *Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment*, in *Studies in Conflict & Terrorism*, 4, 2019, p. 383 ss.;
- A. LAMBERTI, *Libertà di informazione e democrazia. Approccio multilevel e questioni attuali*, in AA.VV., *Spazio di libertà sicurezza e giustizia. A vent'anni dal Consiglio europeo di Tampere* (a cura di A. DI STASI, L.S. ROSSI), Napoli, 2020;
- D.S. LANDES, *Prometeo liberato. La rivoluzione industriale in Europa dal 1750 a oggi*, Torino, 2000;
- M. LANDOLFI, *La Corte di Giustizia UE interviene ancora sulla conservazione e sull'accesso ai dati di traffico e di ubicazione: alcune riflessioni sulla disciplina interna (prima parte)*, in *Studium Juris*, 12, 2021, p. 1481 ss.;
- A. LANG, *Il diritto ad un ricorso effettivo nell'Unione europea*, in AA.VV., *La tutela multilivello dei diritti* (a cura di P. BILANCIA, E. DE MARCO), Milano, 2004;
- M. LANOTTE, *Il requisito dell'indipendenza del pubblico ministero nell'emissione di un ordine europeo di indagine*, in *Cass. pen.*, 3, 2021, p. 1060 ss.;
- G. LATTANZI, *Il dialogo tra le Corti nei casi Melloni e Taricco*, in *Cass. pen.*, 6, 2017, p. 2131B ss.;
- N. LAZZERINI, *La Carta dei diritti fondamentali dell'Unione europea. I limiti di applicazione*, Bologna, 2018;
- N. LE BONNIEC, *L'avis 1/15 de la CJUE relatif à l'accord PNR entre le Canada et l'Union européenne: une délicate conciliation entre sécurité nationale et sécurité numérique*, in *Revue trimestrielle de droit européen*, 3, 2018, p. 617 ss.;
- P. LE JEUNE, *La coopération policière européenne contre le terrorisme*, Bruxelles, 1992;
- C. LE NGUYEN, W. GOLMAN, *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: "Law on the books" vs "law in action"*, in *Computer Law & Security Review*, 40, 2021, Article 105521, p. 1 ss.;
- G. LEBRUN, *De l'utilité de l'article 47 de la Charte des droits fondamentaux de l'Union européenne*, in *Revue trimestrielle des droits de l'homme*, 106, 2016, p. 433 ss.;
- A. LEIPOLD, *How the pretrial process contributes to wrongful convictions*, in *The American Criminal Law Review*, 4, 2005, 1123 ss.;
- K. LENAERTS, *Le traité de Lisbonne et la protection juridictionnelle des particuliers en droit de l'Union*, in *Cahiers de droit européen*, 5-6, 2009, p. 711 ss.;

- G. LEONE, *Trattato di diritto processuale penale*, I, Napoli, 1961;
- C.D. LEOTTA, *La repressione penale del terrorismo a un anno dalla riforma del D.L. 18 febbraio 2015, n. 7, conv. con modif. dalla L. 17 aprile 2015, n. 43*, in *Arch. pen.*, 2016, p. 11 ss.;
- M.C. LIBICKI, *Cyberdeterrence and Cyberwarfare*, Santa Monica (CA), 2009;
- E.T. LIEBMAN, *Giudice naturale e costituzione del giudice*, in *Riv. dir. proc.*, 1964, p. 331 ss.;
- K. LIGETI, G. ROBINSON, *Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?*, in AA.VV., *Vielfact des Strafrechts im internationalen Kontext: Festschrift für Frank Hoüpfel zum 65. Geburtstag* (R. KENT, A. LEHNER eds.), Wien, 2018;
- T. LINARDI, *Sequestro probatorio – il sequestro probatorio e la “copia” dei dati informatici*, in *Giur. it.*, 10, 2019, p. 2286 ss.;
- U. LINDERFALK, *On the Interpretation of Treaties: the Modern International Law as Expressed in the 1969 Vienna Convention on the Law of Treaties*, Dordrecht, 2007;
- V. LOIA, F. ORCIUOLI, *Understanding the composition and evolution of terrorist group networks: A rough set approach*, in *Future Generation Computer Systems*, 101, 2019, p. 983 ss.;
- H. LLOYD-JONES, *Il Prometeo incatenato*, in AA.VV., *Fortuna critica degli autori greci* (a cura di U. ALBINI, F. BORNMANN, M. NALDINI), Firenze, 1977;
- L. LOMBARDI VALLAURI, *Democraticità dell'informazione giuridica e informatica*, in *Informatica e diritto*, 1975, p. 2 ss.;
- F. LONGO, *L'area di libertà, sicurezza e giustizia nella prospettiva politologica*, in AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007;
- E. LORENZETTO, *Le attività urgenti di investigazione informatica e telematica*, in AA.VV., *Sistema penale e criminalità informatica* (a cura di L. LUPARIA), Milano, 2009, p. 143 ss.;
- E. LORENZETTO, *L'assetto delle impugnazioni*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d. lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- E. LORENZETTO, *Continua la saga dei vizi capitali: contraddittorio violato nell'opposizione al riconoscimento dell'ordine europeo di sequestro probatorio*, in *Cass. pen.*, 11, 2020, p. 4093 ss.;
- E. LORENZETTO, *L'ordine europeo di indagine penale: efficienza e garanzie per le acquisizioni probatorie in ambito eurounitario*, in *Cass. pen.*, 3, 2020, p. 1303 ss.;
- M.G. LOSANO, *Dei diritti e dei doveri: anche nella tutela della privacy*, in AA.VV., *La legge italiana sulla privacy. Un bilancio dei primi cinque anni* (a cura di M.G. LOSANO), Roma-Bari, 2001;
- M.G. LOSANO, *Scripta volant: la volatilizzazione dei documenti nell'era digitale*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2020, 17 ss.;
- G. LOZZI, *Lezioni di procedura penale*, Torino, 2018;
- M. LUBERTO, *“Sex-torsion” via web e minaccia a mezzo ransomware: la nuova frontiera del delitto di estorsione*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;

- N. LUCCHI, *La legge Création et Internet: le censure del Conseil constitutionnel*, in *Quad. cost.*, 2, 2010, p. 375 ss.;
- L. LUPÀRIA, *La ricerca della prova digitale tra esigenze cognitive e valori costituzionali*, in AA.VV., *Investigazione penale e tecnologia informatica* (a cura di L. LUPÀRIA, G. ZICCARDI) Milano, 2007;
- L. LUPÀRIA, *Processo penale e scienza informatica: anatomia di una trasformazione epocale*, in AA.VV., *Investigazione penale e tecnologia informatica* (a cura di L. LUPÀRIA, G. ZICCARDI) Milano, 2007;
- L. LUPÀRIA, *I correttivi alle distorsioni sistematiche contenute nella recente legge di ratifica della Convenzione sul Cybercrime*, in AA.VV., *Le nuove norme sulla sicurezza pubblica* (a cura di S. LORUSSO), Padova, 2008;
- L. LUPÀRIA, *La ratifica della Convenzione del Consiglio d'Europa sul cybercrime: profili processuali*, in *Dir. pen. e proc.*, 6, 2008, p. 696 ss.;
- L. LUPÀRIA, *Computer crimes e procedimento penale*, in AA.VV., *Modelli differenziati di accertamento* (a cura di G. GARUTI), Tomo I, Torino, 2011;
- L. LUPÀRIA DONATI, *Privacy, diritti della persona e processo penale*, in *Riv. Dir. proc.*, 6, 2019, p. 1448 ss.;
- L. LUPÀRIA, G. ZICCARDI, *Investigazione penale e tecnologia informatica*, Milano, 2007;
- A. LYLE, *Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism*, in AA.VV., *Open Source Intelligence Investigation: from Strategy to Implementation* (B. AKHGAR, P. S. BAYERL, F. SAMPSON eds.), Heidelberg, 2017;
- A. MAGHAIREH, *Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cyber crime?*, in *International Journal of Cyber Criminology*, 2, 2008, p. 337 ss.;
- T. MAGNO, *Il progetto Evidence e le principali criticità nell'accesso alle prove elettroniche transnazionali in materia penale: quale futuro?*, in *Informatica e diritto*, 2, 2016, p. 152;
- C. MAIOLI, *Dar voce alle prove: elementi di Informatica Forense*, in AA.VV., *Crimine virtuale, minaccia reale. Ict Security: politiche e strumenti di prevenzione*, (a cura di P. POZZI), Milano, 2004;
- A. MALACARNE, *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il "non luogo a provvedere" sulla richiesta del p.m.*, in *Sistema penale*, 5 maggio 2021;
- A. MALACARNE, *"Gravità" dell'ingerenza e "terzietà" dell'organo titolare del potere autorizzatorio: vecchi e nuovi principi in materia di data retention*, in *Riv. It. Dir. e proc. pen.*, 3, 2021, p.1164 ss.;
- A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *Sistema penale*, 8 ottobre 2021, p. 1 ss.;
- S. MANACORDA, *L'armonizzazione dei sistemi penali: una introduzione*, in AA.VV., *La giustizia penale italiana nella prospettiva internazionale*, Atti del Convegno. Courmayeur, 8-10 ottobre 1999, Milano, 2000;

- S. MANACORDA, *Il mandato di arresto europeo nella prospettiva sostanzial-penalistica: implicazioni teoriche e ricadute politico-criminali*, in *Riv. it. Dir. proc. Pen.*, 3, 2004, p. 789 ss.;
- S. MANACORDA, *La consolidation de l'espace de liberté, de sécurité et de justice: vers une "mise à l'écart" du rapprochement pénal*, in *Revue de science criminelle et de droit penal comparé*, 4, 2007, p. 899 ss.;
- S. MANACORDA, *Dalle carte dei diritti a un diritto penale "à la carte"*, in *penalecontemporaneo.it*, 17 maggio 2013;
- S. MANACORDA, *"Doppia pregiudizialità" e Carta dei diritti fondamentali: il sistema penale al cospetto del diritto dell'Unione europea nell'era del disincanto*, in *Riv. it. dir. e proc. pen.*, 2, 2020, p. 572 ss.;
- V. MANES, F. MAZZACUVA, *GDPR e nuove disposizioni penali del codice privacy*, in *Dir. pen. e proc.*, 2, 2019, p. 171 ss.;
- A. MANGIARACINA, *Ancora zone d'ombra in tema di ammissibilità della revisione e indagini difensive svolte all'estero*, in *Giur. It.*, 5, 2009, p. 1244 ss.;
- A. MANGIARACINA, *La circolazione della prova dichiarativa in ambito nazionale ed europeo*, in *Giust. Pen.*, 3, 2010, p. 443 ss.;
- A. MANGIARACINA, *Il procedimento di esecuzione dell'OEI e i margini nazionali di rifiuto*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- A. MANGIARACINA, *L'acquisizione "europea" della prova cambia volto: l'Italia attua la Direttiva relativa all'ordine europeo di indagine penale*, in *Dir. Pen. e Proc.*, 2, 2018, p. 158 ss.;
- A. MANGIARACINA, *Principi generali del mutuo riconoscimento*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MANGIARACINA, sub Art. 696-bis c.p.p., in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MANGIARACINA, sub Art. 696-ter c.p.p., in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MANGIARACINA, sub Art. 696-quater c.p.p., in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MANGIARACINA, sub Art. 696-sexies c.p.p., in AA.VV., *Cooperazione giudiziaria penale*, (a cura di A. MARANDOLA), Milano, 2018;
- A. MANGIARACINA, *Nuovi scenari nell'accesso transfrontaliero alla prova elettronica*, in AA.VV., *Mobilità, sicurezza e nuove frontiere tecnologiche* (a cura di V. MILITELLO, A. SPENA), Torino, 2018;
- A. MANNA, *Erosione delle garanzie individuali in nome dell'efficienza dell'azione di contrasto al terrorismo: la privacy*, in *Riv. it. dir. proc. pen.*, 2004, p. 1022;
- F. MANTOVANI, *Diritto penale. Parte generale*, Milano, 2017;
- D. MANZIONE, *L. 18.3.2008, n. 48 (Criminalità informatica) – Art. 11 – Competenza*, in *Leg. Pen.*, 2008, p. 314 ss.;
- L. MARAFIOTI, *Digital evidence e processo penale*, in *Cass. pen.*, 12, 2011, p. 4509B ss.;
- L. MARAFIOTI, *Armonización y proceso penal europeo: la perspectiva italiana*, in AA.VV., *Miscellanea sul fenomeno giuridico* (a cura di V. MANNINO), Napoli, 2012;

- L. MARAFIOTI, *Orizzonti investigativi europei, assistenza giudiziaria e mutuo riconoscimento*, AA.VV., *L'ordine europeo d'indagine. Criticità e prospettive* (a cura di T. BENE, L. LUPARIA, L. MARAFIOTI), Torino, 2016;
- A. MARANDOLA, *La patologia dell'atto processuale: indirizzi sostanziali vs legalità formale*, in *Dir. pen. e proc.*, 9, 2012, p. 1053 ss.;
- A. MARANDOLA, *Introduzione*, in AA.VV., *Speciale CEDU e ordinamento interno*, *Dir. pen. e proc.*, Milano, 2014, p. 4 ss.;
- A. MARANDOLA, *L'ordine di protezione europeo*, in *Studium Iuris*, 9, 2015, p. 989 ss.;
- A. MARANDOLA, *La tutela dell'identità personale (tra oblio e storicità del fatto)*, in AA.VV., *La vittima del processo. I danni da attività processuale penale* (a cura di G. SPANGHER), Torino, 2017;
- A. MARANDOLA, *La tutela dell'identità personale (informatica), anche del soggetto coinvolto in un processo penale*, in *Proc. pen. e giust.*, 3, 2017, p. 371 ss.;
- A. MARANDOLA, *Sviluppo tecnologico e uso del c.d. captatore informatico*, in *Studium Iuris*, 11, 2017, p. 1285 ss.;
- A. MARANDOLA, *Reciproco riconoscimento alle sentenze penali che irrogano pene detentive o misure privative della libertà personale (d. lg. n. 161/2010)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MARANDOLA, *Reciproco riconoscimento alle decisioni sulle sanzioni pecuniarie (d.lg. n. 37/2016)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MARANDOLA, *Reciproco riconoscimento delle decisioni sulle misure alternative alla detenzione cautelare (d.lg. 36/2016)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MARANDOLA, *Reciproco riconoscimento delle decisioni di sospensione condizionale in vista della sorveglianza delle misure di sospensione condizionale e delle sanzioni sostitutive (d.lg. n. 38/2016)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- A. MARANDOLA, *Giustizia penale e Covid-19 nella legge n. 70 del 2020*, in *Studium Iuris*, 10, 2020, p. 1170 ss.;
- A. MARANDOLA, *I tabulati, un difficile equilibrio tra esigenze di accertamento e tutela di diritti fondamentali*, in *Studium Iuris*, 11, 2021, p. 1328 ss.;
- M.R. MARCHETTI, *Rapporti giurisdizionali con autorità straniera*, in AA.VV., *Compendio di procedura penale* (a cura di G. CONSO, V. GREVI, M. BARGIS) Padova, 2014, p. 1161 ss.;
- M.R. MARCHETTI, *L'assistenza giudiziaria internazionale*, in AA.VV., *Trattato di procedura penale* (diretto da G. UBERTIS, G.P. VOENA), Milano, 2005;
- M.R. MARCHETTI, *Il mandato europeo di ricerca delle prove*, in *Studi in onore di Mario Pisani*, vol. II, *Diritto processuale penale e profili internazionali. Diritto straniero e diritto comparato* (a cura di P. CONSO, E. ZANETTI), Piacenza, 2010;
- M.R. MARCHETTI, *Dalla Convenzione di assistenza giudiziaria in materia penale dell'Unione europea al mandato europeo di ricerca delle prove e all'ordine di indagine penale*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), Milano, 2011;

- M.R. MARCHETTI, *Oltre le rogatorie: i nuovi strumenti per la circolazione degli atti investigativi e delle prove penali*, in AA.VV., *I nuovi orizzonti della giustizia penale europea*. Atti del Convegno nazionale A.S.P.P., Milano, 24-26 ottobre 2014 (a cura di M.R. MARCHETTI), Milano, 2015;
- M.R. MARCHETTI, *Cooperazione giudiziaria: innovazioni apportate e occasioni perdute*, in *Dir. Pen. e Processo*, 12, 2017, p. 1545 ss.;
- M.R. MARCHETTI, *Prospettive di riforma del libro XI c.p.p.*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX convegno nazionale*. Roma, 20-21 ottobre 2016 (a cura di L. KALB), Milano, 2017, p. 27 ss.;
- M.R. MARCHETTI, *Ricerca e acquisizione probatoria all'estero: l'ordine europeo di indagine*, in *Arch. pen., speciale riforme*, 2018, p. 827 ss.;
- M.R. MARCHETTI, *Rapporti giurisdizionali con autorità straniera*, in AA.VV., *Compendio di procedura penale* (a cura di M. BARGIS), Milano, 2020;
- I. MARCHI, *"Emergenza terrorismo": strategie di prevenzione e contrasto anche in prospettiva europea*, in AA.VV., *Diritto penale e modernità. Le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali* (a cura di R. WENIN, G. FORNASARI), Napoli, 2017;
- S. MARCOLINI, *Regole di esclusione costituzionali e nuove tecnologie*, in *Criminalia*, 2006, p. 387 ss.;
- S. MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.*, 7-8, 2010, p. 2855 ss.;
- S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cass. pen.*, 2, 2015, p. 760C;
- S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- S. MARCOLINI, *L'ordine europeo di indagine alla prova dei fatti: prime pronunce in materia*, in *Cass. pen.*, 9, 2019, p. 3370 ss.;
- A. MARI, *Impugnazioni cautelari reali e interesse a ricorrere in caso di restituzione di materiale informatico previa estrazione di copia dei dati*, in *Cass. pen.*, 12, 2017, p. 4303 ss.;
- L. MARINI, *L'evoluzione della disciplina internazionale in materia di terrorismo: qualche spunto recente fra Onu ed Europa*, in *Questione giustizia*, 2, 2017, p. 112 ss.;
- L. MARINI, *Foreign terrorist fighters: verso la revisione della risoluzione 2178 (2014)*, in *penalecontemporaneo.it*, 20 dicembre 2017;
- N.E. MARION, *The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation*, in *International Journal of Cyber Criminology*, 1-2, 2010, p. 699 ss.;
- L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, 1, 2018, p. 61 ss.;
- R. MASTROIANNI, *Diritto dell'Unione europea e processo penale: un'introduzione*, in AA.VV., *L'integrazione europea attraverso il diritto processuale penale* (a cura di R. MASTROIANNI, D. SAVY), Napoli, 2013;
- A. MASUCCI, *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Riv. dir. civ.*, 1, 2004, p. 755 ss.;

- G. MATHISEN, *Nordic Cooperation and the European Arrest Warrant: Intra-Nordic Extradition, the Nordic Arrest Warrant and Beyond*, in *Nordic Journal of International Law*, 1, 2010, p. 1 ss.;
- A. MATTELART, *Storia della società dell'informazione*, Torino, 2002;
- W. MAXWELL, M.W. BRENNAN, A.A. SUR, *Demystifying the US CLOUD Act: Assessing the Law's Compatibility with International Norms and the GDPR*, Washington, 2019;
- G. MAZZA, *Ordine europeo di indagine: la forma soccombe davanti alla sostanziale assenza di pregiudizio*, in *dir. pen. e proc.*, 10, 2021, p. 1343 ss.;
- O. MAZZA, *Il garantismo al tempo del giusto processo*, Milano, 2008;
- O. MAZZA, *Il principio del mutuo riconoscimento nella giustizia penale. La mancata armonizzazione e il mito taumaturgico della giurisprudenza europea*, in *Riv. dir. proc.*, 2, 2009, p. 393 ss.;
- O. MAZZA, *Il principio del mutuo riconoscimento, la mancata armonizzazione e il mito taumaturgico della giurisprudenza europea*, in ID., *Il garantismo al tempo del giusto processo*, Milano, 2011;
- R. MAZZA, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001*, in *La Comunità Internazionale*, 1, 2014, p. 59 ss.;
- F. MAZZACUVA, *La doppia incriminazione e la deroga per i reati di "lista positiva"*, in AA.VV., *L'ordine europeo di indagine penale. Il nuovo volto della raccolta transnazionale delle prove nel d.lgs. n. 108 del 2017* (a cura di M. DANIELE, R.E. KOSTORIS), Torino, 2018;
- R. MEDHI, *Retour sur l'arrêt Melloni: quelques réflexions sur des usages contradictoires du principe de primauté*, in *gdr-elsj.eu*, 29 marzo 2013;
- R. MEGGIATO, *Il lato oscuro della rete. Alla scoperta del Deep Web e del Bitcoin*, Milano, 2014;
- G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in *Cass. pen.*, 1, 2006, p. 265B ss.;
- G. MELILLO, *Il mutuo riconoscimento e la circolazione della prova*, in AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007;
- J.P. MELTZER, *After Schrems II: The Need for a US-EU Agreement Balancing Privacy and National Security Goals*, in *Global Privacy Law Review*, 1, 2021, p. 83 ss.;
- M. MENNA, *Mandato di ricerca della prova e sistemi probatori*, in *Dir. pen. proc.*, 3, 2011, p. 370 ss.;
- D. MESSINEO, *La garanzia del "contenuto essenziale" dei diritti fondamentali. Dalla tutela della dignità umana ai livelli essenziali delle prestazioni*, Torino, 2012;
- V. MILITELLO, *Informatica e criminalità organizzata*, in *Riv. trim. dir. pen. econ.*, 1990, p. 81 ss.;
- C. MILLARD, *Cloud Computing Law*, Oxford, 2021;
- M.F. MIQUELON-WEISMANN, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?*, in *J. Mashall J. Computer & Info L.*, 2, 2005, p. 329 ss.;
- M. MIRTI, *La disciplina giuridica del cyberspace*, in *Opinio Juris*, 23 novembre 2016;
- A. MISSIROLI, *The Dark Side of the Web: Cyber as a Threat*, in *European Foreign Affairs Review*, 2, 2019, p. 142 ss.;

- V. MITSILEGAS, *The Constitutional Implications of Mutual Recognition in Criminal Matters in EU*, in *Common Market Law Review*, 5, 2006, p. 1277 ss.;
- V. MITSILEGAS, *EU Criminal Law*, Oxford, 2009;
- V. MITSILEGAS, *The Symbiotic Relationship Between Mutual Trust and Fundamental Rights in Europe's Area of Criminal Justice*, in *New Journal of European Criminal Law*, 6, 4, 2015, p. 457 ss.;
- V. MITSILEGAS, *EU Criminal Law After Lisbon: Rights, Trust and the Transformation of Justice in Europe*, Oxford, 2018;
- V. MITSILEGAS, *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in *Maastricht Journal of European and Comparative Law*, 3, 2018, p. 263 ss.;
- F.M. MOLINARI, *Questioni in tema di perquisizione e sequestro di materiale informatico*, in *Cass. pen.*, 2, 2012, p. 696 B ss.;
- J. MONAR (ed.), *The institutional dimension of the European Union's area of freedom, security and justice*, Bruxelles, 2010;
- S. MONICI, *Emanate le norme di attuazione della convenzione di assistenza giudiziaria in materia penale del 29 maggio 2000: quali margini operativi in vista dell'(imminente) trasposizione della direttiva sull'ordine europeo di indagine?*, in *Eurojus*, 3 maggio 2017;
- S. MONTALDO, *Internet e commons: le risorse della rete nella prospettiva dei beni comuni*, in *Diritto dell'informazione e dell'informatica*, 2, 2013, p. 287 ss.;
- S. MONTALDO, *La competenza dell'Unione europea ad adottare norme penali ex art. 83, par. 2, TFUE e sue possibili applicazioni*, in *Studi sull'integrazione europea*, 1, 2013, p. 101 ss.;
- S. MONTALDO, *Mandato d'arresto europeo, principio del reciproco riconoscimento e diritti del condannato*, in *Diritti umani e diritto internazionale*, 1, 2013, p. 226 ss.;
- S. MONTALDO, *I limiti della cooperazione in materia penale nell'Unione europea*, Napoli, 2015;
- S. MONTALDO, *Amici mai, odiarsi mai: il controllo sull'applicazione del principio di sussidiarietà alla luce della prassi della Commissione e della Corte di giustizia*, in *Federalismi.it*, 26 giugno 2016, p. 2 ss.;
- S. MONTALDO, *On a Collision Course! Mutual Recognition, Mutual Trust and the Protection of Fundamental Rights in the Recent Case-Law of the Court of Justice*, in *European Papers*, 3, 2016, p. 965 ss.;
- S. MONTALDO, *A caccia di... prove. L'ordine europeo di indagine penale tra complesse stratificazioni normative e recepimento nell'ordinamento italiano*, in *Giur. Pen.*, 11, 2017, p. 1 ss.;
- S. MONTALDO, *La scadenza del termine di recepimento della direttiva 2014/41/UE sull'ordine europeo di indagine penale e la sostituzione delle "disposizioni corrispondenti" della convenzione di assistenza giudiziaria tra gli Stati membri del 2000: spunti per la ricostruzione di un quadro normativo complesso*, in *Il diritto dell'Unione europea*, in *Il diritto dell'Unione europea*, 30 giugno 2017, p. 1 ss.;
- S. MONTALDO, *Framework Decision 2008/909/JHA and Fundamental Rights Concerns: In Search of Appropriate Remedies*, in AA.VV., *The Transfer of Prisoners in the*

- European Union Challenges and Prospects in the Implementation of Framework Decision 2008/909/JHA* (a cura di S. MONTALDO), The Hague, 2020;
- S. MONTALDO, *Framework Decision 2008/909/JHA on the transfer of prisoners in the EU: Advances and challenges in light of the Italian experience*, in *The New Journal of European Criminal Law*, 1, 2020, p. 69 ss.;
- S. MONTALDO, *The cross-border enforcement of probation measures and alternative sanctions in the EU: The poor application of Framework Decision 2008/947/JHA*, in *EU Law Enforcement*, 31 gennaio 2020, p. 1 ss.;
- S. MONTALDO, *The Road Ahead: Proposals for Improving the Implementation of Framework Decision 2008/909/JHA*, in AA.VV., *The Transfer of Prisoners in the European Union Challenges and Prospects in the Implementation of Framework Decision 2008/909/JHA* (a cura di S. MONTALDO), The Hague, 2020;
- S. MONTALDO, L. GROSSIO, *La riforma della disciplina di recepimento del mandato di arresto europeo: il nuovo assetto dei limiti all'esecuzione della richiesta di consegna*, in *Rivista Freedom, Security & Justice: European Legal Studies*, 3, 2021, p. 95 ss.
- A. MONTI, *La nuova disciplina del sequestro informatico*, in AA.VV., *Sistema penale e criminalità informatica* (a cura di L. LUPARIA), Milano, 2009;
- S. MORETTI, voce *Guerra santa*, in *Treccani online*, disponibile al link: [http://www.treccani.it/enciclopedia/guerra-santa_\(Enciclopedia-dei-ragazzi\)/](http://www.treccani.it/enciclopedia/guerra-santa_(Enciclopedia-dei-ragazzi)/);
- P. MOSCARINI, *Naturalità e imparzialità del giudice*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII convegno nazionale. Salerno, 25-27 ottobre 2018* (a cura di L. KALB), Milano, 2019;
- L. MOXLEY, *EU Release e-Evidence Proposal for Cross-Border Data Access*, in www.insideprivacy.com;
- M. MUBIALA, *Contributions à l'étude comparative des mécanismes régionaux africain, américain et européen de protection des droits de l'homme*, in *Afr. J. Int. Comp. Law*, 9, 1997, p. 42 ss.;
- B. MULLER, W.K. RASHBAUM, A. BAKER, A. GOLDMAN, *Prosecutors Describe Driver's Plan to Kill in Manhattan Terror Attack*, in *New York Times*, 1 novembre 2017;
- M. MURCHISON, *Extradition's Paradox: Duty, Discretion, and Rights in the World of Non-Inquiry*, in *Stanford Journal of International Law*, 2, 2007, p. 295 ss.;
- C.C. MURPHY, *The European Evidence Warrant: mutual recognition and mutual (dis)trust?*, in AA.VV., *Crime within the area of Freedom, Security and Justice. A European Public Order* (a cura di C. ECKES, T. KONSTADINIDES), Cambridge, 2011;
- S. MURUSEGAN, I. BOJANOVA (a cura di), *Encyclopedia of Cloud Computing*, Hoboken, 2016;
- U. NANNUCCI, *Le regole di competenza quali norme strumentali al principio del giudice naturale*, in *Dir. pen. e proc.*, 4, 1995, p. 461 ss.;
- B. NASCIMBENE, *Da Schengen a Maastricht: apertura delle frontiere, cooperazione giudiziaria e di polizia*, Milano, 1995;
- B. NASCIMBENE, *Lo spazio di libertà, sicurezza e giustizia a due anni dall'entrata in vigore del Trattato di Lisbona*, in *Dritto, immigrazione e cittadinanza*, 4, 2011, p. 13 ss.;
- NATIONAL INSTITUTE OF STANDARD AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, *The NIST Definition of Cloud Computing*, 2011;

- N. NAVARRO BATISTA, *The development and consolidation of the Area of Freedom, Security and Justice*, in *Revista General de Derecho europeo*, 2017, p. 389 ss.;
- D. NEGRI, *La regressione della procedura penale ad arnese poliziesco (sia pure tecnologico)*, in *Arch. pen.*, 2016, p. 44 ss.;
- D. NEGRI, *Compressione dei diritti di libertà e principio di proporzionalità*, in AA.VV., *Diritti della persona e nuove sfide del processo penale* (a cura di L. KALB), Milano, 2019;
- S. NEGRI, *L'incidenza della Convenzione europea dei diritti dell'uomo sulla cooperazione giudiziaria penale nell'Unione Europea*, in «*Spazio europeo di giustizia e procedimento penale italiano*» (a cura di L. KALB), Torino, 2012;
- S. NEGRI, *La realizzazione dello spazio europeo di libertà, sicurezza e giustizia tra Carta dei diritti fondamentali e CEDU: dalla convergenza alla integrazione tra sistemi?*, in AA.VV., *Spazio europeo e diritti di giustizia. Il capo VI della Carta dei diritti fondamentali nell'applicazione giurisprudenziale* (a cura di A. DI STASI), Napoli, 2014;
- E. NEVEU, *Une société de communication?*, Paris, 1994;
- G. NICASTRO, *Eurojust*, in AA.VV., *Diritto penale europeo e ordinamento italiano*, Milano, 2006;
- S. NICOLIN, *Il mutuo riconoscimento tra mercato interno e sussidiarietà*, Padova, 2005;
- H. NILSSON, *From classical judicial cooperation to mutual recognition*, in *International Review of Penal Law*, 1, 2006, p. 53 ss.;
- M. NINO, *Il rapporto tra la lotta al terrorismo e tutela dei diritti fondamentali nell'esperienza giuridica statunitense*, in AA.VV., *Scritti in memoria di Fulvio Fenucci* (a cura di A. BARBERA, A. LOIODICE, M. SCUDIERO, P. STANZIONE), Soveria Mannelli, 2010;
- M. NINO, *Le prospettive della lotta al terrorismo internazionale dopo la Conferenza di Revisione dello Statuto della Corte Penale Internazionale*, in AA.VV., *Globalizzazione e pluralità delle fonti giuridiche: un duplice approccio. Liber Discipulorum A Dual Approach to Globalization and Legal Pluralism* (a cura di G. ZICCARDI CAPALDO), Napoli, 2012;
- M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012;
- M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Dir. Un. Eur.*, 4, 2014, p. 803 ss.;
- M. NINO, *La sentenza Schrems II della Corte di giustizia UE: trasmissione dei dati personali dall'Unione europea agli Stati terzi e tutela dei diritti dell'uomo*, in *Diritti umani e diritto internazionale*, 3, 2020, p. 733 ss.;
- M. NINO, *The Evolution of the Concept of Territorial Sovereignty. From the Traditional Westphalian System to the State-Peoples Binomial*, in *La comunità internazionale*, 4, 2020, p. 561 ss.;
- M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il diritto dell'Unione europea*, 1, 2021, p. 93 ss.;
- M. NOBILI, sub *Art. 25 comma 1 Cost.*, in AA.VV., *Commentario della Costituzione* (a cura di G. BRANCA, A. PIZZORUSSO), Bologna, 2004;

- A. NOCERA, *Le norme attuative della Convenzione europea di assistenza giudiziaria in materia penale (Bruxelles, 29 maggio 2000)*, in *ilpenalista.it*, 24 maggio 2017;
- A. NOCERA, *Il sindacato giurisdizionale interno in tema di ordine europeo di intercettazione*, in *dir. pen. cont.*, 1, 2018, p. 149 ss.;
- W. NOCERINO, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano, 2021, p. 278 ss.;
- W. NOCERINO, *La nuova (e incompleta) disciplina dei tabulati telefonici in Italia*, in *Intelligence Security Investigation*, 30 novembre 2021;
- W. NOCERINO, *La sorveglianza di massa e i principi della CEDU*, in *Intelligence Security Investigation*, 28 giugno 2021;
- G. NOJEIM, *Cloud Act Implementation Issue*, in *Lawfareblog*, 10 luglio 2018;
- N.I.M. NOVÁKY, *The Invocation of the European Union's Mutual Assistance Clause: A Call for Enforced Solidarity*, in *European Foreign Affairs Review*, 3, 2017, p. 357 ss.;
- S. NUTTAL, *European Political Cooperation*, Oxford, 1992;
- F. NUZZO, *Indicazioni della Corte costituzionale in tema di rogatorie all'estero*, in *Cass. pen.*, 11, 2002, p. 3334 ss.;
- M. O'FLOINN, D. ORMEROD, *Social networking sites, RIPA and criminal investigations*, in *Criminal Law Review*, 10, 2011, p. 766 ss.;
- M. O'FLOINN, D. ORMEROD, *Social networking materials as criminal evidence*, in *Criminal Law Review*, 7, 2012, p. 486 ss.;
- J. ÖBERG, *The legal basis for Eu criminal law harmonisation. A question of federalism?*, in *European law review*, 3, 2018, p. 366 ss.;
- S. OPILIO, *L'ordine europeo di indagine penale*, in AA.VV., *Appunti di cooperazione giudiziaria penale* (a cura di F. FALATO), Napoli, 2019;
- A. ORAKHELASHVILI, S. WILLIAMS (eds.), *40 Years of the Vienna Convention on the Law of Treaties*, London, 2010;
- M. OREFICE, *I big data. Regole e concorrenza*, in *Politica del diritto*, 4, 2016, p. 698;
- R. ORLANDI, *Questioni attuali in tema di processo ed informatica*, in *Riv. dir. processuale*, 1, 2009, p. 135 ss.;
- R. ORLANDI, *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. e proc. pen.*, 2014, p. 1133 ss.;
- U. PAGALLO, *Il diritto nell'età dell'informazione*, Torino, 2015;
- U. PAGALLO, *Profili tecnico-informatici e filosofici*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- A. PAGLIARO, voce *Legge penale nello spazio*, in *Enc. giur.*, XXIII, Milano, 1973;
- C.E. PALIERO, *Dieci anni di "corporate liability" nel sistema italiano: il paradigma imputativo nell'evoluzione della legislazione e della prassi*, in AA.VV., *D.lgs. n. 231: dieci anni di esperienze nella legislazione e nella prassi*, in *Soc.*, 2011, n. spec., p. 5 ss.;
- R. PALLADINO, *Sul diritto all'oblio e la tutela dei diritti fondamentali in internet: ambito di applicazione territoriale e bilanciamento a margine della sentenza Google LLC della Corte di giustizia dell'UE*, in *I diritti dell'uomo*, 3, 2019, p. 543 ss.;
- A. PALMER, *Mutual Legal Assistance: Understanding the Challenges for Law Enforcement in Global Cybercrime Cases*, in *Center for Cyber and Homeland Security at Auburn University*, gennaio 2018, p. 1 ss.;

- L. PALMIERI, voce *Eurojust*, in *Enciclopedia Treccani on line*, [http://www.treccani.it/enciclopedia/eurojust_\(Diritto-on-line\)/](http://www.treccani.it/enciclopedia/eurojust_(Diritto-on-line)/);
- L. PALMIERI, *La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali. Dalla sentenza “Scurato” alla riforma sulle intercettazioni*, in *Dir. pen. cont.*, 1, 2018, p. 59 ss.;
- L. PALMIERI, *La riforma di Eurojust e i nuovi scenari in materia di cooperazione giudiziaria*, Milano, 2019;
- M. PANEbianco, *L’approvazione parlamentare del mandato d’arresto europeo*, in AA.VV., *Mandato d’arresto europeo e garanzie della persona* (a cura di M. PEDRAZZI), Milano, 2004;
- L. PANELLA, *Mandato di arresto europeo e protezione dei diritti umani: problemi irrisolti e “incoraggianti” sviluppi giurisprudenziali*, in *Freedom, Security and Justice: European Legal Studies*, 3, 2017, p. 5 ss.;
- N. PARISI, *Il mandato europeo di ricerca delle prove nel sistema della cooperazione giudiziaria penale fra gli Stati membri dell’Unione*, in *Riv. it. dir. inter. Priv. e proc.*, 2, 2009, p. 327 e ss.;
- N. PARISI, *Riconoscimento reciproco delle decisioni giudiziarie penali, confiance mutuelle e armonizzazione delle garanzie procedurali negli Stati membri dell’Unione europea*, in AA.VV., *Scritti in onore di Ugo Draetta* (a cura di N. PARISI, M. FUMAGALLI MERAVIGLIA, D. RINOLDI, A. SANTINI), Napoli, 2011;
- N. PARISI, *Tecniche di costruzione di uno spazio penale europeo. In tema di riconoscimento reciproco delle decisioni giudiziarie e di armonizzazione delle garanzie procedurali*, in *I quaderni europei*, 2012, p. 5 ss.;
- D.B. PARKER, *Crime by Computer*, New York, 1976;
- PARLAMENTO ITALIANO, COMMISSIONE PER I DIRITTI E I DOVERI RELATIVI AD INTERNET, *Dichiarazione dei diritti in internet*, 28 luglio 2015;
- L. PARLATO, voce *Perquisizioni on-line*, in *Enciclopedia del diritto, Annali*, X, 2017;
- L. PARLATO, *Libertà della persona nell’uso delle tecnologie digitali*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale*, Salerno, 25-27 ottobre 2018, Milano, 2019;
- C. PARODI, *Il recepimento della direttiva 2014/41/UE: le disposizioni in tema di intercettazioni*, in *studiosiprocessopenale.it*, p. 1 ss.;
- C. PARODI, *Ordine europeo di indagine: la disciplina delle intercettazioni*, in *Cass. pen.*, 3, 2020, p. 1314 ss.;
- C. PARODI, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in *ilprocessotelematico.it*, 25 maggio 2021;
- S. PARSHEERA, P. JHA, *The Move Toward Direct Data Access Agreements*, in *Cross-Border Data Access for Law Enforcement: What Are India’s Strategic Options?*, Carnegie Endowment for International Peace, 2020;
- J.T. PARRY, *International Extradition, the Rule of Non-Inquiry and the Problem of Sovereignty*, in *Boston University Law Review*, 2010, p. 1973 ss.;
- I.C. PAȘCA, *The Danger of Islamic Terrorism in Romania*, in *Journal of Eastern-European Criminal Law*, 1, 2016, p. 166 ss.;
- G. PASCUIZZI, *Cyberdiritto. Guida alle banche dati italiane e straniere, alla rete Internet e all’apprendimento assistito da calcolatore*, Bologna, 1995;

- G. PASCUZZI, *Scoperte scientifiche, invenzioni e protocolli relativi a Internet*, in *AIDA*, 5, 1996, p. 161 ss.;
- G. PASCUZZI, voce *Internet (dir. civ.)*, in *Dig. disc. civ.*, Agg., Torino, 2000, p. 225 ss.;
- G. PASCUZZI, *Il diritto dell'era digitale. Tecnologie informatiche e regole privatistiche*, Bologna, 2002;
- G. PASCUZZI, *Il diritto nell'era digitale*, III ed., Bologna, 2016;
- G. PASCUZZI, R. CASO, *I diritti sulle opere digitali*, Padova, 2002;
- A. PASQUERO, *Mutuo riconoscimento delle decisioni penali: prove di federalismo. Modello europeo e statunitense a confronto*, Milano, 2007;
- V. PATANÉ, *Recent Italian Efforts to Responds to Terrorism at the Legislative Level*, in *Journal of International Criminal Justice*, 4, 2006, p. 1166 ss.;
- V. PATANÉ, *Il processo penale nei nuovi scenari dello spazio di libertà, sicurezza e giustizia dell'Unione europea*, in AA.VV., *L'Unione europea dopo il Trattato di Lisbona* (a cura di N. PARISI, V. PETRALIA), Torino, 2011;
- P. PAWLAK, A. MISSIROLI, *Introduction: Trends, Patterns and Challenges for International Cooperation in Cyberspace*, in *European Foreign Affairs Review*, 2, 2019, p. 125 ss.;
- C. PECORELLA, *Truffe online: momento consumativo e competenza territoriale*, in *penalecontemporaneo.it*, 10 febbraio 2012;
- S. PEERS, *Mutual recognition and criminal law in the European Union: has the council got it wrong*, in *Common Market Law Review*, 1, 2004, p. 5 ss.;
- S. PEERS, T. HERVEY, S. KENNER, A. WARD (eds.), *The EU Charter of Fundamental Rights. A Commentary on the European Union Charter of Fundamental Rights*, Oxford, 2014;
- S. PEERS, S. PRECHAL, *Article 52*, in AA.VV., *The EU Charter of Fundamental Rights: A Commentary* (a cura di S. PEERS, T. HARVEY, J. KENNER), Oxford, 2014;
- M. PELLEGRINO, *Cooperazione giudiziaria penale nell'U.E. Dalle origini alla Procura europea*, Padova, 2016;
- A. PERDUCA, *Prove, investigazioni e cooperazione giudiziaria su scala europea*, in AA.VV., *Processo penale e giustizia europea. Omaggio a Giovanni Conso*, Milano, 2010;
- P. PERLINGIERI, *Il diritto civile nella legalità costituzionale, secondo il sistema italo-comunitario delle fonti*, tomo II, Napoli, 2006;
- I. PERNICE, *The Right to Effective Judicial Protection ad Remedies in the EU*, in AA.VV., *The Court of Justice and the Construction of Europe: analyses and Perspectives on Sixty Years of Case law* (A. ROSAS, E. LEVITS, Y. BOT eds.), Berlin, 2013;
- P. PERRI, voce *Computer forensics (indagini informatiche)*, in *Dig. disc. pen.*, Agg. VI, Torino, 2011, p. 100 ss.;
- G. PESTELLI, *D.L. 132/2021: un indiscutibile e inutile aggravio di procedura per tabulati telefonici e telematici*, in *Quotidiano giuridico*, 4 ottobre 2021;
- A. PETERS, A. HINDOCHA, *US Global Cybercrime Cooperation: A Brief Explainer*, in *Third Way*, giugno 2020, p. 1 ss.;
- D. PETRINI, *La responsabilità penale per i reati via internet*, Napoli, 2004;

- R. PEZZUTO, *Accesso transfrontaliero alla prova elettronica nel procedimento penale: la nuova iniziativa legislativa della Commissione europea al vaglio del Consiglio dell'Unione*, in *Dir. pen. cont.*, 1, 2019;
- V.M. PFISTERER, *The Right to Privacy-A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, in *German Law Journal*, 5, 2019, p. 722 ss.;
- B. PIATTOLI, *Cooperazione giudiziaria e pubblico ministero europeo*, Milano, 2002;
- B. PIATTOLI, *Rogatorie internazionali*, in AA.VV., *Rapporti internazionali* (a cura di M.G. AIMONETTO), Torino, 2002;
- G. PICA, voce *Reati informatici e telematici*, in *Dig. disc. pen.*, Agg. I, Torino, 2000, p. 521 ss.;
- G. PICA, voce *Internet (dir. pen.)*, in *Dig. disc. pen.*, Agg. II, Torino, 2004, p. 425 ss.;
- R. PICCIRILLO, *I profili funzionali e strutturali dell'Ordine europeo di indagine penale*, in AA.VV., *L'ordine europeo di indagine. Criticità e prospettive* (a cura di T. BENE-L. LUPARIA, L. MARAFIOTI), Torino, 2016;
- L. PICOTTI, *Problemi penalistici in tema di falsificazione di dati informatici*, in *Il Diritto dell'informazione e dell'informatica*, 1985, p. 939 ss.;
- L. PICOTTI, *Studi di diritto penale dell'informatica*, Verona, 1992;
- L. PICOTTI, *Le "Raccomandazioni" del XV Congresso Internazionale di Diritto penale in tema di criminalità informatica*, in *Riv. trim. dir. pen. econ.*, 1995, p. 1279 ss.;
- L. PICOTTI, *La legge penale*, in AA.VV., *Giurisprudenza sistematica di diritto penale, codice penale, parte generale* (a cura di F. BRICOLA, F. ZAGREBELSKY), Torino, 1996;
- L. PICOTTI, *Profili penali delle comunicazioni illecite via internet*, in *Il Diritto dell'informazione e dell'informatica*, 2, 1999, 320 ss.;
- L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in AA.VV., *Il diritto penale dell'informatica nell'epoca di internet* (a cura di L. PICOTTI), Padova, 2004;
- L. PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'Internet*, 5, 2008, p. 437 ss.;
- L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. e proc.*, 6, 2008, p. 700 ss.;
- L. PICOTTI, *La nozione di «criminalità informatica» e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, 4, 2011, p. 827 ss.;
- L. PICOTTI, *Sicurezza, informatica e diritto penale*, in AA.VV., *Sicurezza e diritto penale* (a cura di M. DONINI, M. PAVARINI), Bologna, 2011;
- L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., p. 35 ss.;
- ID., *Reati informatici, riservatezza e identità digitale*, report presentato al VII Convegno Nazionale dei Professori di Diritto Penale sul tema "Il diritto penale tra recenti modifiche e progetti di riforma", Torino, 9-10 novembre 2018;
- L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- J.P. PIERINI, *Ancora attuale il principio locus regit actum con riguardo alle prove penali acquisite all'estero nel corso di rogatoria "concelebrata"?*, in *Cass. pen.*, 2000, p. 3106 ss.;

- J.P. PIERINI, *Assistenza giudiziaria a favore di autorità straniere e diritto di difesa: è vera incompatibilità?*, in *Cass. pen.*, 2, 2002, p. 1113 ss.;
- S. PIETROPAOLI, *Cyberspazio. Ultima frontiera dell'inimicizia? Guerre, nemici e pirati nel tempo della rivoluzione digitale*, in *Rivista di filosofia del diritto*, 2, 2019, p. 391 ss.;
- G. PINO, *Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica*, 2, 2014, p. 541 ss.;
- A. PINTO, *Giudice naturale e legittima suspicione*, in *Riv. pen.*, 1967, p. 133 ss.;
- M. PISANI, *La garanzia del "giudice naturale" nella Costituzione italiana*, in *Riv. it. dir. e proc. pen.*, 1961, p. 414 ss.;
- M. PISANI, *Criminalità organizzata e cooperazione internazionale*, in *Riv. it. dir. proc. pen.*, 3, 1998, 703 ss.;
- M. PISANI, *In tema di assunzione all'estero delle prove da parte dell'autorità giudiziaria italiana*, in *Riv. it. dir. e proc. pen.*, 2001, p. 557 ss.;
- M. PISANI, *La decisione quadro sul mandato europeo di ricerca delle prove*, in *Riv. it. Dir. proc. pen.*, 1, 2009, p. 479 ss.;
- M. PISANI, *Problemi di prova in materia penale. La proposta di direttiva sull'Ordine Europeo di Indagine*, in *Arch. pen.*, 3, 2011, p. 14 ss.;
- M. PISANI, F. MOSCONI, *Codice delle Convenzioni di estradizione e di assistenza giudiziaria in materia penale*, Milano, 2003;
- E. PISTOIA, *Cooperazione penale nei rapporti tra diritto dell'Unione Europea e diritto statale*, (a cura di E. PISTOIA), Napoli, 2008;
- L. PISTORELLI, *Le Sezioni Unite di fronte alle sfide della modernità: le pratiche di "remotizzazione" delle intercettazioni*, in *Cass. pen.*, 1, 2009, p. 40 ss.;
- M. PITTIRUTI, *Digital evidence e procedimento penale*, Torino, 2017;
- A. PIZZORUSSO, *Giudice naturale*, in *Enc. giu. Treccani*, XVI, Roma, 1989;
- F. POCAR, *L'assistenza giudiziaria internazionale in materia civile*, Padova, 1967;
- M. POELEMANS, *Bilan et perspectives du principe de reconnaissance mutuelle en matière pénale en France*, in AA.VV., *The Future of Mutual Recongnition in Criminal Matters in the European Union* (a cura di G. VERNIMMEN, VAN TIGGELEN, L. SURANO, A. WEYEMBERGH), Bruxelles, 2009;
- G. POI, *Indizi cautelari – la valutazione degli indizi nella fase cautelare: una questione da risolvere alla luce della teoria generale della prova*, in *Giur. it.*, 1, 2017;
- O. POLLICINO, M. BASSINI, *La proposta di Regolamento E-Evidence: osservazioni a caldo e possibili sviluppi*, in *medialaws.ue*, 26 ottobre 2018, p. 1 ss.;
- R. POMAHÁČ, *Soudní dvůr EU: Předávání údajů jmenné evidence cestujících v letecké dopravě z Unie do Kanady*, in *Právní rozhledy: časopis pro všechna právní odvětví*, 21, 2017, p. 761 ss.;
- M.G. PORCEDDA, *Rule of Law and Human Rights in Cyberspace*, in AA.VV., *Riding the digital wave: the impact of cyber capacity building on human development* (eds. P. PAWLAK), EU Institute for Security Studies, Paris, 2014;
- S. PORTESI, *Potential Applications of Advances in Tecnology to Prevention and Response to Cases of Terrorism and Criminality: the Role of Information and Communication Technologies*, in *Cyberspazio e diritto*, 2, 2004, p. 159 ss.;
- C. POUNDER, *The Council of Europe Cyber-Crime Convention*, in *Computers & Security*, 5, 2001, p. 380 ss.;

- L. PRESACCO, *Profili fondamentali del pubblico ministero europeo*, in *Cass. pen.*, 12, 2018, p. 4399 ss.;
- R. PRIEBE, *EuGH beanstandet Fluggastdatenabkommen zwischen der EU und Kanada*, in *Europäische Zeitschrift für Wirtschaftsrecht*, 19, 2017, p.762 ss.;
- L. PRIMICERIO, *Riesaminabilità del decreto di sequestro eseguito per rogatoria all'estero*, in *Cass. pen.*, 10, 2003, p. 2996 ss.;
- D. PULITANÒ, G. DODARO, sub *Art. 3 c.p.*, in AA.VV., *Commentario breve al codice penale* (a cura di G. FORTI, S. SEMINARA, G. ZUCCALÀ), VI ed., Milano, 2017;
- P.J. PULLEN, *Nail in the MLAT Coffin: Examining Alternative Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing*, in *North Carolina Journal of International Law*, 4, 2019, p. 1 ss.;
- S. QUATTROCOLO, *Intelligenza artificiale e giustizia nella cornice della Carta etica europea. Gli spunti per una urgente discussione tra scienze penali e informatiche*, in *La Legislazione penale*, 18 dicembre 2018;
- S. QUATTROCOLO, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Berlino, 2020;
- S. QUATTROCOLO, *Nozioni autonome o variabili? La Corte di giustizia e la definizione di «autorità giudiziaria» e «autorità emittente» nel sistema della cooperazione giudiziaria infraeuropea. Riflessioni a margine di due recenti pronunce*, in *Cass. pen.*, 5, 2021, p. 1792 ss.;
- F. QUILLERE-MAJZOUB, *Le Protocole à la Charte africaine des droits de l'homme et des peuples relatif aux droits de la femme en Afrique: un projet trop ambitieux?*, in *RTDH*, 2007;
- T. RAFARACI, *Lo spazio di libertà, sicurezza e giustizia nel crogiolo della costruzione europea*, in AA.VV., *L'area di libertà, sicurezza e giustizia: alla ricerca di un equilibrio fra priorità repressive ed esigenze di garanzia* (a cura di T. RAFARACI), Milano, 2007;
- T. RAFARACI, *La cooperazione di polizia e giudiziaria in materia penale nell'Unione Europea dopo il trattato di Lisbona*, Milano, 2011;
- T. RAFARACI, *General Considerations on the European Investigations Order*, in AA.VV., *Transnational Evidence and Multicultural Inquiries in Europe* (a cura di S. RUGGERI), Berlino, 2014;
- T. RAFARACI, *Rogatorie*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX convegno nazionale. Roma, 20-21 ottobre 2016* (a cura di L. KALB), Milano, 2017;
- T. RAFARACI, *Brief Notes on the European Public Prosecutor's Office: Ideas, Project and Fulfilment*, in T. RAFARACI, R. BELFIORE (eds.), *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019;
- T. RAFARACI, *Verso una law of evidence dei dati*, in *Dir. Pen. proc.*, 7, 2021, p. 853 ss.;
- G. RAIMONDI, *Editoriale. Spazio di libertà, sicurezza e giustizia, diritti fondamentali e dialogo tra giudici*, in *Freedom, Security & Justice Review*, 2, 2019, p. 2 ss.;
- G. RANALDI, *Processo penale e prova informatica: profili introduttivi*, in *Diritto Pubblico Europeo - Rassegna Online*, 2, 2020;
- M.J. RANGEL DE MESQUITA, Sub art. 47, in AA.VV., *Carta dos direitos fundamentais da União Europeia* (A. SILVEIRA, M. CANOTILHO eds.), Coimbra, Almedina, 2013;

- A. RASI, *Effetti indiretti della Carta dei diritti fondamentali? In margine alla sentenza Commissione c. Polonia (Indépendance de la Cour suprême)*, in *European Papers – European Forum*, 31 luglio 2019;
- G.J. RATTRAY, *An Environmental Approach to Understanding Cyberpower*, in F. KRAMER, S. STARR, L. WENTZ (eds), *Cyberpower and National Security*, Washington (D.C.), 2009;
- E.P. REALE, *Defence Areas and Limits in the Investigations of the European Public Prosecutor*, in T. RAFARACI, R. BELFIORE (eds.), *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019;
- S. RECCHIONE, *Estensione delle rogatorie per l'assunzione della testimonianza del minore: la Corte Costituzionale dichiara infondata la questione, già sussistendo le garanzie invocate dal rimettente*, in *Dir. pen. cont.*, 5, 2018, p. 309 ss.;
- B. REDDING, *The Long Arm of the Law or the Invasive Reach of the American Legal System*, in *International Business Law Journal*, 5, 2007, p. 659 ss.;
- M. REDOLFI, *Anonimato in rete: note tecniche*, in AA.VV., *Sicurezza e anonimato in rete* (a cura di A. MAGGIPINTI, M. IASELLI), Milano, 2005;
- E. RESTA, *Il diritto, la libertà, la tecnica*, in *Riv. crit. dir. priv.*, 1, 2001, p. 79 ss.;
- F. RESTA, *Virtualità del crimine. Dai reati informatici ai cybercrimes*, in *L'informatica nel diritto*, Supplemento a "Giurisprudenza di merito", 2006;
- F. RESTA, *Cybercrime e cooperazione internazionale nell'ultima legge della legislatura*, in *Giur. merito*, 9, 2008, p. 2147B ss.;
- M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico – Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Dir. pen. cont.*, 3, 2016, p. 157 ss.;
- G. RICHERI, *Autostrade dell'informazione*, in *Economia della cultura*, 2, 1994, p. 116 ss.;
- W. RIDGWAY, *Understanding The CLOUD Act's Expansive Reach*, in *Mondaq*, 13 dicembre 2018;
- F. RINALDINI, *Data retention e procedimento penale. Gli effetti della sentenza della Corte di giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore*, in *Giurisprudenza penale web*, 11 maggio 2021;
- D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia*, Napoli, 2010;
- P. RIVELLO, *Tecniche scientifiche e processo penale*, in *Cass. pen.*, 4, 2013, p. 1691B;
- P. RIVELLO, *L'interesse alla richiesta di riesame del provvedimento di sequestro probatorio di materiale informatico*, in *Cass. pen.*, 1, 2018, p. 131 ss.;
- C. RIZCALLAH, *Arrêt «Dorobantu»: mandat d'arrêt européen et exigences minimales relatives aux conditions de détention*, in *Journal de droit européen*, 2, 2020, p. 62 ss.;
- G. ROBINSON, *The European Commission's e-Evidence Proposal*, in *European Data Protection Law Review*, 3, 2018, p. 347 ss.;
- C. RODRÍGUEZ-MEDEL NIETO, *Obtención y admisibilidad en España de la prueba penal transfronteriza. De las comisiones rogatorias a la orden europea de investigación*, Pamplona, 2016;
- S. RODOTÀ, *Persona, libertà, tecnologia. Note per una discussione*, in *D.&Q. pubbl.*, 2005, p. 25 ss.;
- S. RODOTÀ, *La vita e le regole. Tra diritto e non diritto*, Milano, 2009;

- S. RODOTÀ, *Una Costituzione per Internet?*, in *Politica del diritto*, 2, 2010, p. 337 ss.;
- S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Bari, 2014;
- S. RODOTÀ, *Prefazione*, in AA.VV., *Internet, i nostri diritti* (a cura di A. MASERA, G. SCORZA), Bari, 2016;
- M. ROGALSKI, *The European Commission's e-Evidence Proposal – Critical Remarks and Proposals for Changes*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 4, 2020, p. 333 ss.;
- M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, in *Computer Law & Security Review*, 38, 2020, p. 1 ss.;
- R. ROMBOLI, *Il giudice naturale. I. Studio sul significato e la portata del principio nell'ordinamento costituzionale italiano*, Milano, 1981;
- A.D. ROMEO, *Hidden Threat: The Dark Web Surrounding Cyber Security*, in *Northern Kentucky Law Review*, 1, 2016, p. 74 ss.;
- M.^a I. ROMERO PRADAS, *La prueba penal en Europa, una cuestión compleja. La orden europea de investigación como nuevo instrumento de obtención de pruebas en procesos penales transnacionales y su próxima incorporación al Derecho español*, in AA.VV., *Integración europea y justicia penal* (M.^a I. GONZÁLEZ CANO, Directora), Valencia, 2018;
- F. ROMOLI, *Il nuovo volto dell'Europa dopo il Trattato di Lisbona. Un'analisi penalistica "multilivello"*, in *Arch. Pen.*, 1, 2011, p. 166 ss.;
- A. ROSANÒ, *Il nuovo mondo della cooperazione giudiziaria in materia penale nell'Unione Europea: le proposte della Commissione Europea sugli ordini di produzione e conservazione di prove elettroniche (E-Evidence)*, in *La Legislazione penale*, 16 ottobre 2020, p. 1 ss.;
- A. ROSANÒ, *Framework Decision 2008/909/JHA in Context: Interplay with the European Arrest Warrant and (EU) Extradition Law*, in AA.VV., *The Transfer of Prisoners in the European Union Challenges and Prospects in the Implementation of Framework Decision 2008/909/JHA* (a cura di S. MONTALDO), The Hague, 2020;
- E. ROSI, *Criminalità organizzata transnazionale e sistema penale italiano. La convenzione ONU di Palermo*, Roma, 2007;
- E.A. ROSSI, *Gli accordi PNR (Passenger Name Record) nella lotta al terrorismo internazionale. Conseguenze del parere n. 1/15 della Corte di giustizia del 26 luglio 2017 per la legittimità della direttiva n. 2016/681/UE*, in *Diritto comunitario e degli scambi internazionali*, 3, 2018 p. 395 ss.;
- F. ROSSI, *Il processo multifattoriale di radicalizzazione al fondamentalismo "jihadista"*, in *Sistema penale*, 6, 2020, p. 305 ss.;
- F. ROSSI DAL POZZO, *L'Accordo Privacy Shield non è un vero scudo per la privacy: scenari passati e futuri in merito al trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti*, in *Rivista di diritto internazionale*, 4, 2020, p. 1112 ss.;
- M. ROTENBERG, *Schrems II, from Snowden to China: toward a new alignment on transatlantic data protection*, in *European Law Journal: review of European law in context*, 1-2, 2020, p.141 ss.;
- K.A. RUANE, *The Advocacy of Terrorism on Internet: Freedom of Speech Issues and the Material Support Status*, in *Congressional Research Service*, 8 settembre 2016, p. 1 ss.;

- G. RUGANI, *La protezione dei dati nel settore della cooperazione giudiziaria e di polizia in materia penale alla luce della direttiva (UE) 2016/680: frammentazione ed incertezze applicative*, in *Freedom, Security & Justice Review*, 1, 2019, p. 84 ss.;
- A. RUGGERI, *La Corte di giustizia e il bilanciamento mancato (a margine della sentenza Melloni)*, in *Il Diritto dell'Unione europea*, 2, 2013, p. 399 ss.;
- A. RUGGERI, *La dignità dell'uomo e il diritto di avere diritti (profili problematici e ricostruttivi)*, in *Consulta online*, 2, 2018, p. 392 ss.;
- A. RUGGERI, *L'equilibrio nei rapporti tra Corti europee e Corti nazionali: un'autentica quadratura del cerchio possibile solo in prospettiva de iure condendo*, in *Rivista Freedom, Security & Justice: European Legal Studies*, 3, 2021, p. 1 ss.;
- S. RUGGERI, *Introduction to the Proposal of a European Investigation Order: Due Process Concerns and Open Issue*, in AA.VV., *Transnational Evidence and Multicultural Inquiries in Europe* (a cura di S. RUGGERI), Cham-Heidelberg-New York-Dordrecht-London, 2014;
- S. RUGGERI, *Criminal Investigations, Interference with Fundamental Rights and Fair Trial Safeguards in the Proceedings of the European Public Prosecutor's Office. A Human Rights Law Perspective*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018;
- F. RUGGERI, *Le intercettazioni «per instradamento» sul canale internazionale: un mezzo di ricerca della prova illegittimo*, in *Cass. pen.*, 4, 2000, p. 1058 ss.;
- F. RUGGERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cass. pen.*, 6, 2017, p. 2483 ss.;
- F. RUGGERI, *La legge delega in tema di cooperazione penale internazionale: la montagna ha partorito un topolino?*, in *Proc. pen. e giust.*, 2, 2017, p. 315 ss.;
- F. RUGGERI, *Le nuove frontiere dell'assistenza penale internazionale: l'ordine europeo di indagine penale*, in *Proc. pen. e giust.*, 1, 2018, p. 12 ss.;
- F. RUGGERI, *Il libro XI del codice di rito. Guida minima*, in *Cass. pen.*, 5, 2018, p. 1766 ss.;
- F. RUGGERI, *Novità. Il protocollo 16 alla Cedu in vigore dal 1° agosto 2018. La proposta per l'ordine europeo di conservazione o di produzione della prova digitale*, in *Cass. Pen.*, 7-8, 2018, p. 2660 ss.;
- G.M. RUOTOLO, *Hey! You! Get Off My Cloud! Accesso autoritativo alle nuvole informatiche e diritto internazionale*, in *Arch. pen.*, 3, 2013, p. 785 ss.;
- G.M. RUOTOLO, *Il ruolo del consenso del sovrano territoriale nel transborder data access tra obblighi internazionali e norme interne di adattamento*, in *La Comunità internazionale*, 2, 2016, p. 198 ss.;
- G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021;
- G. SABATINI, *La competenza surrogatoria ed il principio del giudice naturale nel processo penale*, in *Riv. it. dir. e proc. pen.*, 1962, p. 941 ss.;
- A. SACCUCCI, *Il Protocollo istitutivo della Corte africana dei diritti dell'uomo e dei popoli, un primo confronto con le altre Corti regionali*, in *Riv. Dir. int.*, 4, 2004, p. 1036 ss.;
- V. SACHETTI, *Il contrasto alla propaganda terroristica online nell'ambito dell'Unione europea: tutela attuale e prospettive future*, in *Eurojus*, 4, 2019, p. 16 ss.;

- A. SACHOULIDOU, *The key elements of the LIBE Committee's compromise proposal on e-evidence: a critical overview through a fundamental rights lens*, in *Global Affairs*, 16 novembre 2021, p. 1 ss.;
- F. SACHWALD, *La Mondialisation comme facteur d'intégration régionale*, in *Politique étrangère*, LXII, 2, 1997, p. 257 ss.;
- A. SAGLIOCCA, *Open Source Intelligence e Deep Web: Scenari Moderni delle Investigazioni Digitali*, in *Cyberspazio e diritto*, 1, 2017, p. 171 ss.;
- L. SALAZAR, *La costruzione di uno spazio di libertà, sicurezza e giustizia dopo il Consiglio europeo di Tampere*, in *Cass. pen.*, 4, 2000, p. 1114 ss.;
- L. SALAZAR, *La nuova Convenzione europea sull'assistenza giudiziaria in materia penale [I parte]*, in *Dir. pen. proc.*, 11, 2000, p. 1534 ss.;
- L. SALAZAR, *La nuova Convenzione europea sull'assistenza giudiziaria in materia penale [II parte]*, in *Dir. pen. proc.*, 12, 2000, p. 1664 ss.;
- L. SALAZAR, *La lotta alla criminalità nell'Unione: passi in avanti verso uno spazio giudiziario comune prima e dopo la Costituzione per l'Europa ed il programma dell'Aja*, in *Cass. Pen.*, 11, 2004, p. 3510 ss.;
- L. SALAZAR, *La costruzione di uno spazio penale comune europeo*, in AA.VV., *Lezioni di diritto penale* (a cura di G. GRASSO, R. SICURELLA), Milano, 2007;
- L. SALAZAR, *Presente e futuro dello Spazio di libertà, sicurezza, e giustizia: dal Piano d'azione dell'Aja alla "visione" della Commissione europea*, in AA.VV., *Per un rilancio del progetto europeo. Esigenze di tutela degli interessi comunitari e nuove strategie di integrazione penale* (a cura di G. GRASSO, R. SICURELLA), Milano, 2008;
- L. SALAZAR, sub art. 82 TFUE, in AA.VV., *Codice dell'Unione europea operativo* (diretto da C. CURTI GIALDINO), Napoli, 2012;
- L. SALAZAR, *Genesi della Convenzione. La tardiva ratifica e la sua attuale operatività*, in AA.VV., *La nuova cooperazione giudiziaria penale. Dalle modifiche al Codice di Procedura Penale all'Ordine europeo di indagine penale* (a cura di M.R. MARCHETTI, E. SELVAGGI – coord. da G. BARROCU), Padova, 2019;
- L. SALAZAR, *La riforma di Eurojust e i suoi riflessi sull'ordinamento italiano*, in *Dir. pen. cont.*, 1, 2019, p. 44 ss.;
- L. SALAZAR, *La cooperazione giudiziaria penale nell'Unione ai tempi della Brexit*, in *Sistema penale*, 3, 2020, p. 185 ss.;
- O. SALLAVACI, *Rethinking Criminal Justice in Cyberspace: The EU E-Evidence Framework ad a New Model of Cross-Border Cooperation in Criminal Matters*, in AA.VV., *Policing in the Era of AI and Smart Societies* (H. JAHANKHANI, B. AKHGAR, P. COCHRANE, M. DASTBAZ eds.), Cham, 2020;
- I. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv. it. dir. e proc. pen.*, 2, 2017, p. 747 ss.;
- B. SANDFUCHS, *The Future of Data Transfers to Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II*, in *Gewerblicher Rechtsschutz und Urheberrecht International*, 3, 2021 p. 245 ss.;
- M.A. SANDULLI, *Proporzionalità*, in *Dizionario di diritto pubblico*, V, Milano, 2006;
- S. SANTINI, *L'Unione europea compie un nuovo passo nel cammino della lotta al terrorismo: una prima lettura della Direttiva 2017/541*, in *dir. pen. cont.*, 7-8, 2017, p. 13 ss.;

- F. SANTORO, *Cooperazione internazionale in materia di criminalità informatica*, Roma, 2011;
- N. SANZ MULAS, *Las sociedades paralelas como cantera del yihadismo*, in *El terrorismo en la actualidad: un nuevo enfoque político criminal*, dir. da A.I. Pérez Cepeda, coord. da M. Ruiz Arias, Valencia, 2018;
- C. SARZANA DI SANT'IPPOLITO, *La Convenzione europea sulla cybercriminalità*, in *Dir. pen. e proc.*, 4, 2002, p. 509 ss.;
- C. SARZANA DI SANT'IPPOLITO, *La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa*, in *Criminalità informatica*, 12, 2008, p. 1562 ss.;
- C. SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Milano, 2010;
- H. SATZGER, *Is mutual recognition a viable general path for cooperation?*, in *New Journal of European Criminal Law*, 1, 2019, p. 44 ss.;
- V.M. SBRESCIA, *Le comunicazioni elettroniche tra tecnologia e regolazione*, in *Riv. it. dir. pubbl. comunit.*, 5, 2011, p. 1207 ss.;
- G. SCACCIA, *Proporzionalità e bilanciamento tra diritti nella giurisprudenza delle Corti europee*, in *Riv. AIC*, 3, 2017, p. 1 ss.;
- A. SCALFATI, *Note minime su cooperazione investigativa e mutuo riconoscimento*, in *Proc. pen. e giust.*, 2, 2017, p. 217 ss.;
- M. SCAPARONE, *Procedura penale*, vol. II, Torino, 2008, p. 418 ss.;
- B. SCHAFER, S. MASON, *The Characteristics of Digital Evidence*, in S. MASON, *Electronic Evidence*, London, 2012;
- N.M. SCHALLMOSER, *The European Arrest Warrant and Fundamental Rights. Risks of Violations of Fundamental Rights through the EU Framework Decision in Light of the ECHR*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2, 2014, p. 146 ss.;
- A.N. SCHUPACK, *The Arab-Israel Conflict and Civil Litigation Against Terrorism*, in *Duke Law Journal*, 1, 2010, p. 207 ss.;
- P.M. SCHWARTZ, *Legal Access to the Global Cloud*, in *Columbia Law Review*, 6, 2018, p. 1755 ss.;
- C. SCHWARZENEGGER, *Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 – Am Beispiel des Hackings, der unrechtmässigen Datenbeschaffung und der Verletzung des Fernmeldegeheimnisses*, in AA.VV., *Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag* (eds. A. DONATSCH, M. FORSTER, C. SCHWARZENEGGER), Zürich, 2002;
- R. SCIARRONE, *Processi di globalizzazione e criminalità organizzata*, in AA.VV., *Potere politico e globalizzazione* (a cura di P. FANTOZZI), Catanzaro, 2004;
- SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE (SWGDE), INTERNATIONAL ORGANIZATION ON DIGITAL EVIDENCE (IOCE), *Digital Evidence: Standards and Principles*, in *Forensic Science Communications*, 2, 2000;
- Z. SECCHI, *Le novità introdotte dalla Convenzione 9 maggio 2000 in tema di assistenza giudiziaria penale fra gli Stati membri dell'Unione europea*, in *Doc. giust.*, 6, 2000, p. 1108 ss.;

- N. SEITZ, *Transborder Search: A new perspective in law enforcement?*, in *International Journal of Communications Law & Policy*, 9 – Special Issue in Cybercrime, 2004, p. 9 ss.;
- C. SELLARS, *Schrems II and Standard Contractual Clauses – the Advocate-General's Opinion*, in *Computer Law Review International*, 1, 2020, p. 29 ss.;
- E. SELVAGGI, *Criminalità transnazionale e cooperazione giudiziaria internazionale*, in AA.VV., *Criminalità transnazionale fra esperienze europee e risposte penali globali*. Atti del III Convegno Internazionale promosso dal Centro Studi Giuridici “Francesco Carrara”. Lucca, 24-25 maggio 2002, Milano, 2005;
- E. SELVAGGI, *Cooperazione giudiziaria veloce ed efficace*, in *Guida al diritto*, 16, 19 aprile 2008, p. 72 ss.;
- E. SELVAGGI, *Task force operativa 24 ore al giorno*, in *Guida al diritto*, 16, 19 aprile 2008, p. 74 ss.;
- E. SELVAGGI, *La circolare del Ministero della Giustizia sul c.d. ordine europeo di indagine*, in *Dir. pen. cont.*, 11, 2017, p. 287 ss.;
- E. SELVAGGI, *Quel “restyling” che facilita la ricerca di chi è latitante*, in *Guida al diritto*, *Il Sole 24ore*, 45, 4 novembre 2017, p. 66 ss.;
- E. SELVAGGI, *Va “in soffitta” l’atto di exequatur della Corte d’Appello*, in *Guida al diritto*, 45, 4 novembre 2017, p. 73 ss.;
- E. SELVAGGI, *L’ordine europeo di indagine – EIO: come funziona?*, in *Cass. Pen.*, 1, 2018, p. 44B ss.;
- S. SEMINARA, *La pirateria su internet e il diritto penale*, in AIDA. *Annali italiani del diritto d’autore, della cultura e dello spettacolo*, 5, 1996, p. 183 ss.;
- M. SERAFINI, *PlayStation e Isis, cosa sappiamo delle comunicazioni del Califfato*, in *Corriere della sera*, 27 novembre 2015;
- L. SERRANÒ, *“Torture e violenze sessuali in diretta sui minori nel dark web”: lo scoprono i carabinieri di Siena*, in *La Repubblica*, 15 luglio 2020;
- E. SEVERINO, *Il destino della tecnica*, Milano, 1998;
- P. SFAMENI, *Responsabilità patrimoniale e vicende modificative dell’ente*, in AA.VV., *Responsabilità “penale” delle persone giuridiche* (a cura di A. GIARDA, E.M. MANCUSO, G. SPANGHER, G. VARRASO), Milano, 2007;
- E. SHARPSTON, *The future of the area of freedom, security and justice*, in M. DOUGAN, S. CURRIE (eds.), *50 years of the European treaties*, Oxford, 2009;
- T. G. SHIPLEY, A. BOWKER, *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Waltham, 2014;
- J. SHURSON, *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*, in *International Journal of Law and Information Technology*, 28, 2020, p. 167 ss.;
- U. SIEBER, *The International Handbook on Computer Crime*, Portsmouth, 1986;
- U. SIEBER, (ed.), *Information Technology Crime*, Köln, 1994;
- U. SIEBER, *Straftaten und Strafverfolgung im Internet: Gutachten C zum 69. Deutschen Juristentag*, München, 2012;
- U. SIEBER, P. BRUNST, *Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions*, Strasbourg, 2007;

- S. SIGNORATO, *Le misure di contrasto in rete al terrorismo: black list, inibizione dell'accesso ai siti, rimozione del contenuto illecito e interdizione dell'accesso al dominio internet*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo* (a cura di R. KOSTORIS, F. VIGANÒ), Torino, 2015;
- S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino, 2018;
- G. SILVESTRI, *La dignità umana come criterio di bilanciamento dei valori costituzionali*, in *Studi in onore di Pierfrancesco Grossi*, Milano, 2012;
- G. SILVESTRI, *L'individuazione dei diritti della persona*, in AA.VV., *Diritti della persona e nuove sfide del processo penale. Atti del XXXII Convegno nazionale ASPP – Salerno, 25-27 ottobre 2018* (a cura di L. KALB), Milano, 2019;
- D. SIMON, *Applicabilité des accords entre l'Union européenne et le Royaume du Maroc au territoire du Sahara occidental: Acte II*, in *Europe*, 4, 2018, p. 6 ss.;
- D. SIMON, *Mandat d'arrêt européen. Droits fondamentaux dans l'État d'émission*, in *Europe. Actualité du droit de l'Union européenne*, 2, 2021, p. 54 ss.;
- M. SIMONATO, *Deposizione della vittima e giustizia penale. Una lettura del sistema italiano*, Padova, 2014;
- M. SIMONATO, *Reciproco riconoscimento in materia penale e vie di ricorso: la prima sentenza della CGUE sull'ordine europeo di indagine*, in *europeanlawblog.it*, 1 aprile 2020;
- A. SINAGRA, P. BARGIACCHI, *Lezioni di diritto internazionale pubblico*, Milano, 2019;
- D. SIRACUSANO, F. SIRACUSANO, *Le prove, il procedimento probatorio e il processo*, in AA.VV., *Diritto processuale penale* (a cura di G. DI CHIARA, V. PATANÈ, F. SIRACUSANO), Milano, 2018;
- F. SIRACUSANO, *Tra mutuo riconoscimento e armonizzazione preventiva: quali prospettive per la circolazione della prova dichiarativa nell'ambito dell'Unione europea?*, in *Arch. pen.*, 1, 2012, p. 201 ss.;
- F. SIRACUSANO, *La prova informatica transnazionale: un difficile «connubio» fra innovazione e tradizione*, in *Proc. pen. e giust.*, 1, 2017, p. 178 ss.;
- F. SIRACUSANO, *Prove informatiche*, in AA.VV., *Investigazioni e prove transnazionali. Atti del XXX convegno nazionale. Roma, 20-21 ottobre 2016* (a cura di L. KALB), Milano, 2017;
- F. SIRACUSANO, *Tra semplificazione e ibridismo: insidie e aporie dell'Ordine europeo di indagine penale*, in *Arch. Pen.*, 2, 2017, p. 1 ss.;
- F. SIRACUSANO, *The European Investigation Order for Evidence Gathering Abroad*, in *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office* (a cura di T. RAFARACI, R. BELFIORE), Cham, 2019;
- V. SKOURIS, *Développements récents de la protection des droits fondamentaux dans l'Union européenne: les arrêts Melloni et Åkerberg Fransson*, in *Il Diritto dell'Unione europea*, 2, 2013, p. 229 ss.;
- D. SIMON, *Coup de tonnerre dans le monde du numérique. La Cour de justice prononce l'invalidité du «bouclier de protection de la vie privée» à propos des transferts de données personnelles vers les États-Unis*, in *Europe: actualité du droit communautaire*, 8-9, 2020, p. 5 ss.;

- N.A. SMUHA, *Towards the EU Harmonization of Access to CrossBorder E-Evidence: Challenges for Fundamental Rights & Consistency*, in *European Criminal Law Review*, 1, 2018, 83 ss.;
- I. SOBRINO GARCÍA, *Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos*, in *Revista de Derecho Comunitario Europeo*, 68, 2021, p. 227 ss.;
- E. SOMMA, “Naturalità” e “precostituzione” del giudice nell’evoluzione del concetto di legge, in *Riv. it. dir. e proc. pen.*, 1963, p. 797 ss.;
- E. SOMMARIO, *The Status of Foreign Fighters under International Humanitarian Law*, in A. DE GUTTRY, F. CAPONE, C. PAULUSSEN (eds.), *Foreign Fighters under International Law and Beyond*, The Hague, 2016;
- M. SOSSAI, *Foreign Terrorist Fighters: una nozione ai confini del diritto internazionale*, in *federalismi.it*, 25 settembre 2015;
- C. SOTIS, *La perspective d’un droit pénal communautaire*, in AA.VV., *L’intégration pénale indirecte: Interactions entre droit pénal et coopération judiciaire au sein de l’Union européenne* (a cura di G. GIUDICELLI-DELAGÉ, D. MANACORDA), Paris, 2006;
- G. SOULIER, *Le théâtre et le procès*, in *Droit et société*, (117/118), 1991, p. 1 ss.;
- A. SPADARO, *Gli effetti costituzionali della c.d. “globalizzazione”. Storia di una “metamorfosi”: dalla sovranità dei popoli nazionali alla sovranità dell’opinione pubblica (e della finanza) internazionali*, in *Politica del diritto*, 3, 1998, p. 447 ss.;
- P. SPAGNOLO, *I presupposti e i limiti dell’ordine di indagine europeo nella procedura passiva*, in AA.VV., *La nuova cooperazione giudiziaria penale* (a cura di M.R. MARCHETTI, E. SELVAGGI), Milano, 2019;
- P. SPAGNOLO, *La Nuova cooperazione giudiziaria penale: mutuo riconoscimento e tutela dei diritti fondamentali*, in *Cass. pen.*, 3, 2020;
- G. SPANGHER, *La rimessione dei procedimenti*, I, *Precedenti storici e profili di legittimità costituzionale*, Milano, 1984;
- G. SPANGHER, *Il “giusto processo” penale*, in *Studium Iuris*, 2000, p. 256 ss.;
- G. SPANGHER, *Le misure cautelari*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), III, 2015;
- G. SPANGHER, *Le prove informatiche*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- G. SPANGHER, *Covid-19: nel disastro si vede chiaro*, in *Penale diritto e procedura*, 21 aprile 2020;
- G. SPANGHER, *Introduzione allo studio del processo penale*, Pisa, 2020;
- G. SPANGHER, *Il difficile governo della complessità*, in *Intelligence Security Investigation*, 20 giugno 2021;
- G. SPECCHIO, *Analisi di contesto del cyberspace (I parte)*, in *Sicurezza & Giust.*, 3, 2019, p. 11;
- J.R. SPENCER, *The Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility: the Reaction of one British Lawyer*, in *Zeitschrift für Internationale Strafrechtsdogmatik*, 9, 2010, p. 602 ss.;
- J. SPENCER, *Il principio del mutuo riconoscimento*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;

- A. SPERINI, *I Modelli Sistemici del jihadismo: aspetti evolutivi in chiave anti-sistema*, in AA.VV., *Comprendere il terrorismo. Spunti interpretativi di analisi e metodologie di contrasto del fenomeno* (a cura di R. RAZZANTE), Pisa, 2019;
- F. SPIEZIA, *Il coordinamento giudiziario sovranazionale: problemi e prospettive alla luce della nuova decisione 2009/426/GAI che rafforza i poteri di Eurojust*, in *Cass. pen.*, 5, 2010, p. 1991;
- F. SPIEZIA, *Coordinamento investigativo delle indagini ed Eurojust*, in AA.VV., «Spazio europeo di giustizia» e procedimento penale italiano. *Adattamenti normativi e approdi giurisprudenziali* (a cura di L. KALB), Torino, 2012;
- F. SPIEZIA, *La cooperazione giudiziaria internazionale e lo spazio di giustizia europeo*, in AA.VV., *Procedura penale. Teoria e pratica del processo* (diretto da G. SPANGHER, A. MARANDOLA, G. GARUTI, L. KALB), IV, *Le impugnazioni. Esecuzione penale. Rapporti giurisdizionali con autorità straniere* (a cura di L. KALB), Torino, 2015;
- F. SPIEZIA, *Il Pubblico Ministero Europeo e i suoi rapporti con Eurojust*, in *penalecontemporaneo.it*, 29 maggio 2018;
- F. SPIEZIA, *The European Public Prosecutor's Office – How to Implement the Relations with Eurojust?*, in *Eucrim*, 2018, p. 130 ss.;
- F. SPIEZIA, *Attacco all'Europa*, Milano, 2020;
- G. STAMPANONI BASSI, *Acquisizione dei tabulati telefonici: anche la Corte di Assise di Napoli esclude una applicazione diretta della sentenza CGUE del 2 marzo 2021 (C-746/18)*, in *Giurisprudenza penale web*, 17 giugno 2021;
- A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2019;
- C.M.S. STEEL, *Stolen Identity Valuation and Market Evolution on the Dark Web*, in *International Journal of Cyber Criminology*, 1, 2019, p. 70 ss.;
- R. STEFANOVA-KAMISHEVA, *Zashtita na osnovnite prava na choveka pri izpalnenie na evropeyskata zapoved za arest*, in *Evropeyski praven pregled*, 6, 2013, p. 163 ss.;
- J. STERLING, *Philosophical and Legal Challenges in the Context of Copyright and Digital Technology*, *IIC*, 5, 2000;
- K. STERN, *La Carta dei diritti fondamentali dell'Unione europea. Riflessioni sulla forza vincolante e l'ambito di applicazione dei diritti fondamentali codificati nella Carta*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 6, 2014, p. 1235 ss.;
- J. E. STIGLITZ, *La globalizzazione che funziona*, Torino, 2006; ID., *Bancarotta. L'economia globale in caduta libera*, Torino, 2010;
- A.M. STILE, *The Instruments of the Former third pillar in the Lisbon era: towards an Integrated Judicial Control in the Area of Security, Liberty and Justice*, in *New Journal of European Criminal Law*, 4, 2015, p. 482 ss.;
- M. STOHL, *Dr. Strangeweb: Or How They Stopped Worrying and Learned to Love Cyber War*, in T.M. CHEN, L. JARVIS, S. MACDONALD (eds.), *Cyberterrorism. Understanding, Assessment, and Response*, New York, 2014;
- A. STONE SWEET, J. MATTHEWS, *Proportionality Balancing and Global Constitutionalism*, in *Columbia Journal of Transnational Law*, 47, 2008, p. 73 ss.;

- C. STORTI, *La Rogatoria Internazionale nei Codici dell'Unificazione Italiana (1861-1930)*, in AA.VV., *Atti del VII Convegno di Studi – La circolazione della prova nell'UE e la tutela degli interessi finanziari* (a cura di L. A. BANA, L. CAMALDO), Milano, 2011;
- A. STRANDBAKKEN, *The Nordic Answer to the European Arrest Warrant: The Nordic Arrest Warrant*, in *Eucrim*, 3-4, 2007, p. 138 ss.;
- G. STROZZI, *Diritto dell'Unione europea*, V ed., Torino, 2017;
- G. SUFFIA, *Geografia delle cyberwars: uomini e Stati alla prova dello spazio digitale*, Milano, 2018;
- D. ŠUŠNJAR, *Proportionality, Fundamental Rights and Balance of Powers*, Leiden-Boston, 2010;
- D.J.B. SVANTESSON, Q.C.F. GERRY, *Access to Extraterritorial Evidence: The Microsoft Cloud Case and beyond*, in *Computer Law and Security Review*, 4, 2015, p. 478 ss.;
- T. SWIFT, *What is the 'Deep Web'? And Other Questions About the Shadowy Virtual World of Silk Road*, in *Baltimore Sun Online*, 3 ottobre 2013;
- P. SWIRE, *Comments on Australian Legislation to Enable the Negotiation of a U.S. CLOUD Act Executive Agreement*, in *Cross-Border Data Forum*, 11 maggio 2020;
- P. SWIRE, J.D. HEMMINGS, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, in *N.Y.U. Annual Survey of American Law*, 4, 2016, p. 687 ss.;
- P. SWIRE, J.D. HEMMINGS, *Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act*, in *Lawfare*, 13 settembre 2018;
- P. SWIRE, J. HEMMINGS, S. VERGNOLLE, *A Mutual Legal Assistance Case Study: The United States and Francia*, in *Wisconsin International Law Journal*, 2, 2017, p. 323 ss.;
- J. SYLVESTRE BERGÉ, S. GRUMBACH, V. ZENO-ZENCOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, 2, 2018, p.149;
- C. TAORMINA, *Giudice naturale e processo penale*, Roma, 1972;
- C. TAORMINA, *Procedura penale*, Torino, 2015;
- E. TEROLLI, *Privacy e protezione dei dati personali UE vs. USA. Evoluzioni di diritto comparato e il trasferimento dei dati dopo la sentenza "Schrems II"*, in *Il diritto dell'informazione e dell'informatica*, 1, 2021, p. 49 ss.;
- A. TESTAGUZZA, *Digital forensics. Informatica giuridica e processo penale*, Padova, 2014;
- V.M. THELMA, *Elementi probatori acquisiti dal privato in territorio straniero*, in *Proc. pen. e giust.*, 5, 2020, p. 1073 ss.;
- C. THIELE, *Ist der Datentransfer in die USA am Ende? - Zur Unzulässigerklärung des EU Privacy Shield - Analyse der Entscheidung EuGH 16. 7. 2020, C-311/18 mit Praxistipps*, in *JusIT, IT-Recht, Rechtsinformation, Datenschutz*, 70, 2020, p. 196 ss.;
- M. TIBERI, *L'instradamento delle telefonate straniere: una prassi discutibile*, in *Cass. pen.*, 3, 2004, p. 959 ss.;
- G. TIBERI, *Le nuove fonti del diritto nella cooperazione giudiziaria in materia penale dopo il Trattato di Lisbona e il loro impatto sull'ordinamento interno*, in AA.VV., *La cooperazione di polizia e giudiziaria in materia penale nell'Unione europea dopo il Trattato di Lisbona* (a cura di T. RAFARACI), Milano, 2011;

- K. TIEDEMANN, *L'europeizzazione del diritto penale*, in *Riv. it. Dir. proc. Pen.*, 1, 1998, p. 8;
- A. TINOCO PASTRANA, *L'ordine europeo di indagine penale*, in *Proc. pen. e giust.*, 2, 2017, p. 346 ss.;
- A. TINOCO PASTRANA, *La transposición de la orden europea de investigación en materia penal en el ordenamiento español*, in *Rivista Freedom, Security & Justice: European Legal Studies*, 3, 2018, 116 ss.;
- A. TINOCO PASTRANA, *The Proposal on Electronic Evidence in the European Union*, in *Eucrim*, 1, 2020, p. 46 ss.;
- A. TINSLEY, *The Reference in Case C-396/11 Radu: When does the Protection of Fundamental Rights Require Non-execution of a European Arrest Warrant?*, in *European Criminal Law Review*, 2012, p. 338 ss.;
- A. TIZZANO, *Brevi note sul "terzo pilastro" del trattato di Maastricht*, in *Dir. Un. Eur.*, 2, 1996, p. 391 ss.;
- G. TODARO, *Restituzione di bene sequestrato, estrazione di copia, interesse ad impugnare: revirement delle Sezioni Unite*, in *Dir. pen. cont.*, 11, 2017, p. 157 ss.;
- S. TOGNAZZI, *Criminalità informatica e cooperazione internazionale: verso il secondo Protocollo addizionale alla Convenzione di Budapest*, in *Dir. pen. proc.*, 8, 2021, p. 1032 ss.;
- V. TONDI, *L'accesso transfrontaliero all'elettronic evidence, tra esigenze di effettività e tutela dei diritti*, in *Dir. pen. cont.*, 2, 2019, p. 452 ss.;
- V. TONDI, *La disciplina italiana in materia di data retention a seguito della sentenza della Corte di giustizia UE. Il tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema penale*, 7 maggio 2021;
- P. TONINI, *Prova scientifica e contraddittorio*, in *Dir. pen. Proc.*, 9, 2003, p. 1459 ss.;
- P. TONINI, *Documento informatico e giusto processo*, in *Dir. pen. e proc.*, 4, 2009, p. 401 ss.;
- P. TONINI, *L'evoluzione delle categorie tradizionali: il documento informatico*, in AA.VV., *Cybercrime* (diretto da A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA), Milano, 2019;
- P. TONINI, C. CONTI, *Il diritto delle prove penali*, Milano, 2014;
- P. TONINI, C. CONTI, *Manuale di procedura penale*, Milano, 2021;
- F. TORIELLO, *I principi generali del diritto comunitario*, Milano, 2000;
- M. TORRE, *Aspetti giuridici e tecnici relativi al trattamento della prova digitale nel processo penale. La prova informatica nella legge 18 marzo 2008, n. 48*, in *Informatica e diritto*, 1-2, 2015, p. 65 ss.;
- L. TOSONI, *Rethinking Privacy in the Council of Europe's Convention on Cybercrime*, in *Computer Law & Security Review*, 24, 2018, p. 1197 ss.;
- S. TOSZA, *All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order*, in *New Journal of European Criminal Law*, 2, 2020, p. 164 ss.;
- X. TRACOL, *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record Data between the EU and Canada*, in *Computer Law & Security Review*, 34, 2018, p. 830 ss.;

- X. TRACOL, *“Schrems II”: the return of the privacy shield*, in *Computer law & security review*, 39, 2020, p. 1 ss.;
- X. TRACOL, *Chapter V of Regulation (EU) 2018/1725 on transfers of personal data by Union institutions and bodies to third states and international organisations*, in *ERA Forum*, 4 agosto 2021;
- TRANSBORDER GROUP, *Transborder Access and Jurisdiction: What Are the Options?*, Discussion Paper No T-CY(2012)3, Cybercrime Convention Committee, Council of Europe, 6 dicembre 2012;
- F. TRAPPELLA, *Il provvedimento che attua la Convenzione di Bruxelles del 2000: una lunga gestazione e un destino incerto*, in *Proc. pen. e giust.*, 1, 2018, p. 17 ss.;
- T. TREVES, *La giurisdizione nel diritto penale internazionale*, Padova, 1973;
- N. TRIGGIANI, *Le investigazioni difensive*, Milano, 2002;
- N. TRIGGIANI, *In divenire la disciplina dei rapporti con autorità straniere: appunti sulla l. 21 luglio 2016, n. 149*, in *penalecontemporaneo.it*, 5 ottobre 2016;
- N. TROCKER, *Il valore costituzionale del “giusto processo”*, in AA.VV., *Il nuovo articolo 111 della Costituzione e il giusto processo civile* (a cura di M. G. CIVININI E C.M. VERARDI), Milano, 2001;
- M. TROGU, *Sorveglianza e “perquisizioni” online su materiale informatico*, in AA.VV., *Le indagini atipiche* (a cura di A. SCALFATI), Torino, 2014;
- M. TROGU, *Ordine europeo di indagine penale (d. lg. n. 108/2017)*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- P. TROISI, voce *Mandato di arresto europeo*, in *Treccani – Diritto on line*, 2014;
- P. TRONCONE, *La tutela penale del nuovo documento dematerializzato tra vicende novative e nuove aspirazioni sistematiche*, in *Riv. pen.*, 2008, p. 1277 ss.;
- Y. TURIANSKYI, *Africa and Europe: Cyber Governance Lessons*, in *South African Institute of International Affairs*, gennaio 2020, p. 10 ss.;
- S. TURKLE, *La vita sullo schermo. Nuove identità e relazioni sociali nell’epoca di Internet*, Milano, 1997;
- V. TZORTZI, *I shediazomeni symfonia PNR-EE-Kanatha paraviazei ta themeliodi dikaïomata: paratiriseis*, in *Elliniki Epitheorisi Evropaïkou Dikaïou*, 2017, p. 461 ss.;
- A. UBALDI, *Intercettazioni ambientali all’estero: microspia in auto senza rogatoria*, in *Dir. & giustizia*, 131, 2018, p. 8 ss.;
- G. UBERTIS, *“Naturalità” e “precostituzione” del giudice nell’evoluzione del concetto di legge*, in *Riv. it. dir. e proc. pen.*, 1963;
- G. UBERTIS, *“Naturalità” del giudice e valori socio-culturali nella giurisdizione*, in *Riv. it. dir. e proc. pen.*, 1977, p. 1058 ss.;
- G. UBERTIS, *La prova penale. Profili giuridici ed epistemologici*, Torino, 1995;
- G. UBERTIS, *Sistema di procedura penale. Principi generali*, Torino, 2013;
- G. UBERTIS, *“Prova indiziaria”. Ossimoro o ridondanza da evitare*, in *Argomenti di procedura penale*, Milano, 2016;
- G. UBERTIS, *Considerazioni generali su investigazioni e prove transnazionali*, in *Cass. pen.*, 1, 2017, p. 49B ss.;
- G. UBERTIS, *Equità e proporzionalità versus legalità processuale: eterogenesi dei fini?*, in *Arch. pen.*, 2, 2017, p. 390 ss.;

- UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE (UNICRI), *La criminalità informatica e i rischi per l'economia e le imprese a livello italiano ed europeo*, Torino, 2014;
- UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC), *Comprehensive Study on Cybercrime, Draft*, New York, 2013;
- G. VACIAGO, *Internet e crimini informatici*, in AA.VV., *Computer Crimes. Casi pratici e metodologie investigative dei reati informatici* (a cura di M.L. PICCINNI, G. VACIAGO), Bergamo, 2008;
- C. VALENTINI, *L'acquisizione della prova tra limiti territoriali e cooperazione con autorità straniere*, Padova, 1998;
- W. VAN BALLEGOOGIJ, P. BÀRD, *Mutual recognition and individual rights. Did the Court get it right?*, in *New Journal of European Criminal Law*, 4, 2016, p. 439 ss.;
- F. VANORIO, *Il contrasto al terrorismo globale tra esigenze di prevenzione e di tutela dei diritti fondamentali*, in *Questione giustizia*, 5 gennaio 2021;
- G. VARRASO, *Il procedimento per gli illeciti amministrativi dipendenti da reato*, Milano, 2012;
- G. VASSALLI, *Il diritto alla prova nel processo penale*, in *Riv. It. Dir. proc. pen.*, 1968;
- V. VASTA, *Tracciamento elettronico e tabulati telefonici: anche l'Italia a rischio condanna?*, in *Riv. it. dir. e proc. pen.*, 2, 2018, p. 985 ss.;
- A. VEDASCHI, *The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15 The European Court of Justice on the EU-Canada Passenger Name Record Agreement: ECJ, 26 July 2017, Opinion 1/15*, in *European Constitutional Law Review*, 14, 2018, p. 410 ss.;
- A. VENEGONI, *Rogatorie*, in *Cass. pen.*, 5, 2017, p. 393 ss.;
- A. VENEGONI, *Procura europea – EPPO*, in AA.VV., *Cooperazione giudiziaria penale* (a cura di A. MARANDOLA), Milano, 2018;
- N. VENTURA, *Ratifica della Convenzione di Budapest e iniziativa investigativa della polizia giudiziaria*, in *Giust. pen.*, 1, 2008, p. 226 ss.;
- G. VERNIMMEN, VAN TIGGELEN, L. SURANO, A. WEYEMBERGH (eds.), *The future of mutual recognition in criminal matters in the European Union*, Bruxelles, 2009;
- J.A.E. VERVAELE, *The anti-terrorist legislation in the US; inter arma silent leges?*, in *European Journal of Crime, Criminal Law and Criminal Justice*, 2, 2005, p. 201 ss.;
- J.A.E. VERVAELE, *Il progetto di decisione quadro sul mandato di ricerca della prova*, in AA.VV., *Prova penale e Unione europea, Atti del Convegno "L'armonizzazione della prova penale nell'Unione europea". Facoltà di Giurisprudenza dell'Università di Bologna. 18-19 aprile 2008* (a cura di G. ILLUMINATI), Bologna, 2009;
- J.A.E. VERVAELE, *Foreign (terrorist) fighters: combattenti, terroristi o solo nemici?*, in *Riv. it. dir. e proc. pen.*, 4, 2018, p. 1875 ss.;
- F. VIGANÒ, *Obblighi di adeguamento al diritto UE e "controlimiti": la Corte costituzionale spagnola si adegua, bon gré mal gré, alla sentenza dei giudici di Lussemburgo nel caso Melloni*, in *penalecontemporaneo.it*, 9 marzo 2014;
- F. VIGANÒ, *Minaccia dei "lupi solitari" e risposta dell'ordinamento: alla ricerca di un delicato equilibrio tra diritto penale, misure di prevenzione e tutela dei diritti fondamentali della persona*, in AA.VV., *Il nuovo "pacchetto" antiterrorismo* (a cura di R. KOSTORIS, F. VIGANÒ), Torino, 2015;

- D. VIGONI, *Dalla rogatoria all'acquisizione diretta*, in AA.VV., *Rogatorie penali e cooperazione giudiziaria internazionale* (a cura di G. LA GRECA, M.R. MARCHETTI), Torino, 2003;
- D. VILAS ÁLVAREZ, *The Material Competence of the European Public Prosecutor's Office*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018, p. 25;
- U. VILLANI, *Istituzioni di diritto dell'Unione europea*, Bari, 2017;
- U. VILLANI, *Istituzioni di diritto dell'Unione europea*, Bari, 2020;
- M.E. VILLIGER, *Commentary on the 1969 Vienna Convention on the Law of Treaties*, Leiden, 2009;
- M.E. VILLIGER, *The 1969 Vienna Convention on the Law of Treaties: 40 Years after*, in *Collected Courses of the Hague Academy of International Law*, 2009, p. 9 ss.;
- O. VILLONI, G. DE AMICIS, *Il Protocollo della Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea fatta a Bruxelles il 29 maggio 2000*, in *Cass. pen.*, 1, 2002, p. 421 ss.;
- A. VITALE, *La nuova disciplina delle ispezioni e delle perquisizioni in ambiente informatico o telematico*, in *Dir. dell'internet*, 5, 2008, p. 507 ss.;
- V.H. VON HEINEGG, *Legal Implications of Territorial Sovereignty in Cyberspace*, in C. CZOSSECK, R. OTTIS, K. ZIOLKOSKI (eds.), *NATO 4th International Conference on Cyber Conflict*, 2012, Tallin;
- M.L. WADE, *The European Public Prosecutor: Controversy Expressed in Structural Form*, in T. RAFARACI, R. BELFIORE (eds.), *EU Criminal Justice. Fundamental Rights, Transnational Proceedings and the European Public Prosecutor's Office*, Berlino, 2019;
- I. WALDEN, *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*, in AA.VV., *Privacy and Security for Cloud Computing* (S. PEARSON, G. LEE eds.), Heidelberg, 2012;
- I. WALDEN, *Law Enforcement Access to Data in Clouds*, in AA.VV., *Cloud Computing Law* (C. MILLARD ed.), Oxford, 2013;
- A. WANG, *Silk Road: The "eBay" for Narcotics*, in *The Epoch Times*, 6 giugno 2011;
- A.M. WEBER, *The Council of Europe's Convention on Cybercrime*, in *Berkley Technology Law Journal*, 1, 2003, p. 425 ss.;
- F. WEBSTER, *Theories of the information society*, London, 1995;
- B. WESTON, R.A. LUKES, K. HNATT, *Regional Human Rights Regime. A Comparison and Appraisal*, in *Vanderbilt JTL*, 29, 1987, p. 587 ss.;
- A. WEYEMBERGH, *Storia della cooperazione*, in AA.VV., *Manuale di procedura penale europea* (a cura di R.E. KOSTORIS), Milano, 2019;
- S. WHITE, *Towards a Decentralized European Public Prosecutor's Office*, in *New Journal of European Criminal Law*, 1-2, 2013, p. 23 ss.;
- D. WICKI-BIRCHLER, *The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime?*, in *Int. Cybersecur. Law Rev.*, 1, 2020, p. 63 ss.;
- I. WIECZOREK, *The EPPO Draft Regulation Passes the First Subsidiarity Test: An Analysis and Interpretation of the European Commission's Hasty Approach to National Parliament's Subsidiarity Arguments*, in *German Law Journal*, 2015, p. 1247 ss.;

- C. WILLIAMS, *The european Evidence Warrant: the proposal of the European Commission*, in AA.VV., *Dealing with european evidence in criminal proceedings: national practice and European Union policy* (Proceedings of ERA /Crown Prosecution Service Conference – AGIS Project), 18-20 novembre 2004, ERA – Forum, Trier, 2005;
- A.K. WOODS, P. SWIRE, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, in *Lawfare*, 6 febbraio 2018;
- F. ZACCHÈ, sub Art. 25 Cost., in AA.VV., *Codice di procedura penale commentato* (a cura di A. GIARDA, G. SPANGHER), tomo I, Milanofiori Assago, 2017;
- G. ZAGREBELSKY, *Connessione e giudice naturale*, in AA.VV., *Connessione di procedimenti e conflitti di competenza* (Atti del Convegno di studio svoltosi a Trieste-Grignano, 3-5 ottobre 1975), Milano, 1976;
- V. ZAGREBELSKY, *L'istituzione del Procuratore europeo in rapporto alle esigenze dell'equo processo*, in <http://www.europeanrights.eu>, 2014, p. 54 ss.;
- M. ZALNIERIUTE, *Developing a European Standard for International Data Transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *The Modern Law Review*, 6, 2018, p. 1046 ss.;
- E. ZANETTI, *Nasce l'Agenzia dell'Unione europea per la cooperazione giudiziaria penale*, in *Proc. pen. e giust.*, 2, 2019, p. 302 ss.;
- N. ZANON, F. BIONDI, *Il sistema costituzionale della magistratura*, Bologna, 2006;
- E. ZAPPALÀ, F. SIRACUSANO, *I rapporti giurisdizionali con autorità straniere*, in AA.VV., *Diritto processuale penale* (a cura di G. DI CHIARA, V. PATANÈ, F. SIRACUSANO), Milano, 2013;
- A. ZÀRATE CONDE, M. PRADA RODRIGUEZ, *Transactions and "Simplified Procedures" in the Framework of the European Public Prosecutor's Office. A National Perspective*, in L. BACHMAIER WINTER (ed.), *The European Public Prosecutor's Office. The Challenges Ahead*, Berlino, 2018;
- G. ZICCARDI, *La libertà di espressione in Internet al vaglio della Corte Suprema degli Stati Uniti*, in *Quad. Cost.*, 1, 1998, p. 123 ss.;
- G. ZICCARDI, *Hacker. Il richiamo della libertà*, Milano, 2011;
- G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015;
- G. ZICCARDI CAPALDO, M. NINO, *Sistema ONU di contrasto al terrorismo e deficit delle garanzie procedurali e processuali*, in AA.VV., *Studi in onore di Modestino Acone*, vol. I, Napoli, 2010;
- P. ZIMBARDO, *L'effetto Lucifero. Cattivi si diventa?*, Milano, 2008;